UNIVERSITÉ DE SHERBROOKE
Faculté de Génie
Département de Génie Électrique et Informatique
Electrical and Computer Engineering Department

UNE ARCHITECTURE DE SERVICES SUR DEMANDE POUR LES COMMUNICATIONS SANS FILS VEHICULAIRE

AN ON-DEMAND SERVICE ARCHITECTURE FOR WIRELESS VEHICULAR NETWORKS

Philosophae Doctor (Ph.D.) Thesis

Etienne S CORONADO

Jury : Dr. Soumaya CHERKAOUI
Dr. Christer AHLUND
Dr. Brahim CHAIB-DRAA
Dr. Ahmed KHOUMSI

Sherbrooke (Québec), Canada 16 Août 2010

Library and Archives Canada

Published Heritage Branch

395 Wellington Street
Ottawa ON K1A 0N4
Canada

Bibliothèque et
Archives Canada

Direction du
Patrimoine de l'édition

395, rue Wellington
Ottawa ON K1A 0N4
Canada

Your file Votre référence
ISBN: 978-0-494-70633-6
Our file Notre référence
ISBN: 978-0-494-70633-6

Dedication

To God, my parents, brothers and friends

ABSTRACT

Vehicular Networks (VN) or VANETS has become a cutting-edge topic in the development of innovative solutions for the automotive industry and of special interest to transit management authorities. Well known examples of the potential benefits of enabling communications in vehicles is fostering a better driving by reducing the risk of accidents on the road. Besides the transmission of safety messages among vehicles in the vicinity, the development of non-safety applications will allow the delivery of information services to potential users willing to request them in on-demand basis. To provide such type of services, major challenges need to be tackled to offer secure and reliable communication in anonymous and sometimes hostile communication environments on the roads. These challenges cover security, billing and accounting issues to provide a secure access to services.

The objective of this thesis work is to propose a service architecture for on-demand services in vehicular environments. A key point to keep a robust information service supply, stands in the capacity to provide and manage security mechanisms which comprise authentication and authorization of subscribers following a temporary subscription model. These features, along with privacy mechanisms, will offer to the communicating peers a secure way to mutually access and exchange information even if no previous knowledge of each other is available. Policies of service providers can regulate the supply of information services according to the subscribers' profiles. Providers can also define the implementation of accountability models in the form of metering and billing schemes appropriate for VANETS. This will result in the implementation of incentive and collaborative mechanisms to foster service delivery among vehicles.

Keywords: Service Architecture, Security, Provisioning, VANETS

RÉSUMÉ

Les Réseaux véhiculaires (VN) ou VANETS sont devenus un sujet d'avant-garde dans le développement de solutions innovatrices pour l'industrie automobile. Rendre possibles les communications véhiculaires promeut une meilleure conduite tout en réduisant le risque d'accidents sur la route. Outre la transmission de messages de sécurité entre les véhicules, d'autres types d'applications pourraient être conçus pour fournir des services d'information aux utilisateurs potentiels. Des défis majeurs ont besoin cependant d'être abordés pour offrir une communication sur la route sécurisée et fiable dans des environnements anonymes et quelquefois hostiles aux communications. Ces défis sont des problèmes de sécurité, de facturation jusqu'à des problèmes de comptabilité pour fournir un accès sécurisé et fiable aux services offerts sur la route. L'objectif de ce travail de thèse est d'explorer et proposer une architecture de services pour les services sur-demande dans les environnements véhiculaires. Un point clé pour offrir des services informationnel robustes est la capacité de fournir et gérer les mécanismes de sécurité qui comprennent l'authentification et l'autorisation d'abonnés. Ces caractéristiques, conjointement avec les mécanismes de préservation du caractère privé des communications, offriront aux usagers une manière sécurisée d'accéder et d'échanger des informations. Les politiques de fournisseurs de service peuvent réglementer l'approvisionnement de services d'information selon les profils des abonnés. Les fournisseurs peuvent définir aussi l'implémentation de modèles de responsabilité sous forme de mécanismes de mesure et de facturation appropriés pour les VANETS. Ceci aura pour résultat l'implantation de mécanismes de collaboration pour promouvoir la délivrance de services à travers des véhicules participants.

Mots clés : l'Architecture de Services, Sécurité, Facturation, VANETS

ACKNOWLEDGEMENTS

I want to thank my parents for their support and their unconditional love along this time. Also I want to thank my brother Adrian for his encouragement and advice through my studies. Thanks to my brother Christian and his wife Maggie for their advice and prayers.

I want to express my gratitude to my supervisor Dr Soumaya Cherkaoui for her patience and guidance along this project. Without her support and direction, I would not have been able to complete this project.

Special thanks to the Canadian Network of Centres of Excellence and to the National Science and Engineering Research Council for the financial support that made possible the completion of this work and for the exceptional opportunity to network with other researchers and expand my knowledge horizons in the annual Highly Qualified Personnel (HQP) Conferences. Thanks to all the participants and collaborators of the Project F-202 Vehicle Communications and Applications.

Thanks to my colleague Balkrishna Gukhool for the good times and conversations we had in INTERLAB. Also thanks to Hansa Gukhool, Bruno Gagnon, Carlos and Norma Mendoza, Antonio Ramirez, Luc Bissette, Marc and Sophie Coulomb, Tommy Gagnon, Melanie Gagne, Erika Davis, Selene Lau and to all my friends from Campus pour Christ for their prayers.

Table of Contents

LIST OF TABLES

LIST OF FIGURES

LIST OF ACRONYMS

AAA : Authentication Authorization and Accounting

ACE : Application Characterization Environment

AH : Authentication Header

AODV : Ad Hoc On Demand Distance Vector routing

AODV: An On Demand Vector

AP : Access Point

AR : Access Router

ART : Average Response Time

ASL : Application Sublayer

CA : Certificate Authority

CRL : Certificate Revocation List

CVIS : Cooperative Vehicle-Infrastructure System

DB : Database

DH : Diffie-Hellman algorithm

DHCP : Dynamic Host Configuration Protocol

DoS : Denial-of-Service

DSDV : Destination-Sequence Distance Vector routing

DSRC : Dedicated Short Range Communication

ESP : Encapsulation Security Payload

ETC : Electronic Toll Collection

FTP : File Transfer Protocol

GA : Governmental Authority

GL : Group Leader

GPS : Global Positioning System

GSM : Global System for Mobile communications

HMAC : Hash-based Message Authentication Code

HMI : Human Machine Interface

HTTP : HyperText Transfer Protocol

IP : Internet Protocol

IPv6 : IP version 6

LBS : Location Based Services

LHR : Load Hybrid Routing

MSW : Message Switch

MIPv6 : Mobile IP version 6

NM : Network Management

OBE : On-board Equipment

OBU : On-board Unit

OEM : Original Equipment Manufacturers

OSGI : Open Service Gateway Initiative

PA : Private Authority

PID : Pseudonym Identification

PKI : Public Key Infrastructure

PMK : Pairwise Master Key

PSID : Provider Service Identifier

PST : Provider Service Table

QoS : Quality of Service

RSA : Rivest Shamir Adleman algorithm

RSE : Roadside Equipment

RSU : Roadside Unit

SHA : Secure Hash Algorithm

SLA : Service Level Agreement

SMR : Session to Mobility Ratio

SP : Service Provider

TCP : Transport Control Protocol

TGS : Ticket Grant Server

TGT : Ticket Grant Ticket

TPD : Tamper Proof Device

UDP : User Datagram Protocol

UMTS : Universal Mobile Telecommunications System

V2I : Vehicle-infrastructure

V2V : Vehicle-to-Vehicle

VANETS : Vehicular Ad Hoc Networks

VN : Vehicular Networks

VRT : Variation Response Time

VSCC : Vehicle Safety Communication Consortium

WAVE : Wireless Access for Vehicular Environments

WiMAX : Worldwide Interoperability for Microwave Access

WLAN : Wireless Local Area Network

WME : WAVE Management Entity

WSIE : WAVE Service Information Element

WSM : WAVE Short Message

ZRP : Zone Routing Protocol

CHAPTER 1

INTRODUCTION

Vehicular Ad Hoc Networks (VANETS) are intended to enable short and medium range transmission for vehicle-to-vehicle or vehicle-roadside communications. One main service that is enabled by VANETS is safety applications. The potential benefit associated to vehicle safety applications is to reduce the number of accidents on the road. This is because communications makes possible the propagation of collision avoidance warnings, current road conditions, triggered messages about unexpected events, traffic information and the exchange of driving information among vehicles for an optimal drive. Given the nature of safety applications, the exchange of this type of information needs to be distributed in a real-time basis since related situations are safety critical or life threatening. Nevertheless the advantages of safety applications, the development of a communication technology, namely IEEE 802.11p [Antipolis, 2005], capable to support vehicular messages is still not concluded since the initial efforts 10 years ago. Contributors such as official transport authorities, academia and automotive industry have been involved in technical working groups to consolidate the release of the wireless vehicular standard. Given the intrinsic complexity in deploying vehicular networks and other external constraints such as legal issues, the completion of the technology roadmap has been delayed. This resulted in some inconvenience such as, for example, the deferral of the goal targeted by the European Union Transit Commission which aimed to reduce the number of accidents occurred in the year 2000 to half of that number by the year 2010 [TERM, 2002].

Besides the implementation of wireless technology for safety purposes, another trend of potential applications increasingly being considered is the deployment of commercial non-safety services. This type of applications can be thought of distributed mobile applications provided possibly by different service providers that use shared communication channels on the road. This means that providers might use different business models to offer multiple services that exceed the limited range of services commonly offered by a single network operator. In this context, extended cooperative services represent a key opportunity to exploit that has got a huge potential of economic profitability since different providers might be able to offer their applications through open standard platforms. Thus in a competitive market, providers would be distinguished by the type of value-added services offered to their potential users.

One of the main challenges in the deployment of vehicular networks is that it might require the installation of expensive infrastructure strategically distributed on the road. In most of the cases, the coverage range will depend on the density of potential users' demands; for example, highly populated areas such as cities would require more coverage capacity than sparsely inhabited rural areas. Once the infrastructure is available, the array of commercial services broadcasted on the road can be extensive. One can think of Internet access, vehicle infotainment, navigation assistance for transportation logistics management and high speed automatic toll collection services.

1.1 Context and problematic

Service provisioning models for VANETS need to consider the convergence of heterogeneous service applications whose success depends on the implementation of robust architectures. Heterogeneous service applications are considered to be open architectures from different service providers which can be integrated on the same wireless access infrastructure. These architectures must be able to maintain their overall performance when facing real life scenarios on the road. In many cases, communications in such a highly 'open' model can be subjected to many security threats that can hinder the reliability and the survivability of services provider businesses. For example, potential anonymous attackers might be present and represent a potential risk to any ongoing service delivery. Additionally, resources availability can be compromised by "lying" users which send false emergency messages to have some kind of advantage on the road, or any sort of communication attack that attempts to disrupt services. For these reasons, it can be assumed that any communication that takes place in an open public area and in the presence of non-trusted or anonymous peers can potentially experience communication attacks. In other words, any vehicle in the surrounding area is a non-trusted entity and can be labelled as a potential attacker.

A question that raises then is how a service offered on the road could be granted and delivered to a user in a secure manner in untrustworthy surroundings. In a vehicular context, it is legitimate to assume that any registered vehicle on the road can have the capability to initiate service requests to any service infrastructure. Furthermore, current trends in the automobile and telecommunication industries suggest vehicles must be capable to communicate among them and with the road infrastructure even if no previous communication has been set up before. This implies that the exchange of messages must be supported by non-trusted entities with a significant risk of presenting forwarding misbehavior. As the nature of traffic flows suggests, it becomes evident that one important issue in VANETS deals with dynamic and highly mobile drivers' patterns and which could join accessible wireless networks in a transient or sometimes unpredictable manner.

Based on the above, crucial challenges need to be tackled concerning security, privacy of information and charging operations of on-road services. In general, a key point to maintain robust information services relies in the capacity to provide and manage security mechanisms which comprise authentication and authorization of users. These features, along with privacy mechanisms, need to be offered to the communicating peers to mutually access and exchange information. The security features can be adapted to the vehicle network domain but with the appropriate strategies for their implementation in highly dynamic environments. The supply of information services on the service providers side can also be regulated according to users' profiles. Depending on those profiles, it is possible to classify the type of service model into a compulsory subscription model or an on-demand registration model. In a compulsory subscription model, the subscriber is required to be registered in the provider's databases and to follow access control regulations, get the appropriate permissions and be subjected to service policies. In an on-demand registration model, no previous subscription is needed and the service request and use of services will last as long as the communication link between the subscriber and the wireless infrastructure is established. However, challenging issues arise concerning security and billing capabilities in highly dynamic networks. Most of on-demand services offered on the road can be considered as informative; for instance, a provider can advertise its services through the roadside infrastructure to potential customers, i.e. current sales in department stores or a gas station advertising its oil prices.

Given the aforementioned background context, the objective of this work is that:

> ***"The proposed service architecture must guarantee security, authentication and privacy features in order to establish a service session between an unknown transitory vehicular user and a service provider on the road in an acceptable delay given normal vehicular mobility."***

For the rest of this work, a user is considered to be attached to a specific vehicle in a one-to-one relationship.

In this work, security features address the generation of session keys by the service architecture for the user and the service provider. Session keys will protect the delivery of any kind of services for an ongoing session. Authentication capabilities are based on the validation of disclosed public key certificates through Certificate Revocation Lists (CRL) which detect and disable potential compromised certificates by verifying their most current revocation status. Privacy features, are related to the generation of pseudonyms during the establishment of a session between the user and the service provider. Though there is certain level of privacy granted to the user, full liability must be preserved throughout the service delivery process, assuring non-repudiation characteristics to maintain accountability of the communicating parties.

1.2 Proposed solution

This thesis work proposes security, privacy and incentive approaches that can be implemented in VANETS in a spontaneous on-demand service scenario. The work identifies some key assumptions relevant to the development of service models for VANETS as follows.

1. Hybrid architectures will coexist to provide vehicular-to-vehicular and vehicular-infrastructure communications on the road. Heterogeneous wireless access technologies can be deployed and support seamless interoperation on the road.

2. Multiple heterogeneous service providers can coexist to support a vast variety of services announced by the roadside infrastructure.
3. Multiple authorities can support the operation of district regions. Collaboration among different transit authorities might be required, as well as, international transit authorities reinforcing global mobility of vehicles in geographical areas, i.e. North American and European Union trade regions.
4. Governmental authorities are the entities appointed to assign official credentials and certificates to vehicles. This regulation is similar to the procedures followed in conventional license plate registers.
5. A district region can hold private and official transit entities but governmental authorities have prime control of the infrastructure and its corresponding management.

The key concerns that have been identified in the implementation of a service architecture which guarantees a secure service delivery can be summarized in the following questions and for which corresponding solutions are addressed along this research work.

1. Can a non-trusted vehicle get access to an on-road service without being registered previously to access a provider and how can this service be securely delivered?
   In a dynamic environment such as the one experienced in vehicular networks, open public service architectures need to offer the possibility to deliver services to potential users without previously being registered or subscribed. This issue is addressed in chapter 4 section 4.2 where spontaneous on-demand services are explained. The second part of this question regarding the way secure services are delivered is covered in the secure model addressed in chapter 4 section 4.3 where session attributes are securely dispatched between a corresponding user and a provider. This proposal is complemented with a district service architecture defined in chapter 5 section 5.4 and which was published in the International Journal of Autonomous and Adaptive Communication Systems – IJAACS 2009 [Coronado and Cherkaoui, 2009].
   The analytical model of the service architecture was studied in detail and three types of protocols in an extended district service architecture were defined depending on the

vehicular scenario. The work was published in the Wiley's International Journal in Security and Communication Networks 2009 [Coronado and Cherkaoui, 2009].

2. How can a non-trusted vehicle be charged for a service advertised on the road?
   This concern is addressed in Chapter 5 section 5.6 where charging operations can be supported by a district service domain.
3. In an ad-hoc environment, how can services be delivered to the requester if multi-hop communication among non trusted vehicles is required?
   To tackle the challenge of promoting participation of peer vehicles in a multi-hop environment, it might be necessary to define a set of incentive mechanisms for the delivery of services through intermediate nodes. This concern is addressed in Chapter 5 section 5.7 where collaboration among vehicles is defined through the issuance of incentives to active participating vehicles.

In summary, the service architecture must be able to issue temporary session keys for the potential user and the service provider. These keys must be valid only during the session. The dispatch of session keys must be done once verification of user's certificates and the available credit takes place. Additionally, policy control and authorization tasks have to be done for resource assignation purposes.

Mobility must be supported by the interaction of neighboring service architectures, when a service session is active and the access to the network must be given in the new service architecture domain. The architecture uses the premise that service architectures are controlled and managed by official authorities defined according to their geographic location.

1.3 Thesis Contribution

The main contribution of this work is to propose a service architecture which allows access to spontaneous on-demand services for transient mobile vehicles. The architecture consists of a set of main elements and protocols that provide security, billing, and session management capabilities when a request of a service is executed by the potential user. As a result, this service architecture facilitates the provisioning of services broadcasted on the road throughout the establishment of the necessary session parameters between the service provider and the potential user. The main contributions of this work are enlisted below:

- The proposition of a service district domain managed by district authorities that supports spontaneous on-demand services.
- The definition of the service parameters for on-demand services.
- The definition of a service request protocol in a single hop environment (SHI-RQ).
- The definition of a service request protocol to allow scalability in multiple district domain environments (EC-RQ)
- The definition of billing mechanisms for spontaneous on-demand requests.
- The definition of an incentive collaboration scheme for multi-hop communications.
- The definition of a service request protocol in a multi-hop environment (MHI-RQ).

The contributions of this thesis foster the deployment of non-safety applications along the roadside for traveling vehicles. Different business models can be developed around the proposed architecture that would allow any transitory vehicle to retrieve any announced service on the road. This is possible through the verification of public certificates and credentials disclosed by the potential user at the current service architecture on the road. This premise is based on the assumption that public certificates are issued and constantly monitored by official transit authorities. Information through inter-district domains is possible through a dedicated transit network. Finally, affordability of services must be checked based on banking credentials provided by the potential user.

1.4 Thesis outline

This thesis document is divided into two main parts. The first one includes introductory concepts and a review of literature related to the thesis project. First, a technical description of DSRC (Dedicated Short Range Communication) is given, DSRC being the main wireless vehicular technology under standardization. Second, some references to initiatives in the communication and automotive industry are given in Chapter 2. In Chapter 3, some security concepts and existing approaches for vehicular environments are addressed. Subsequent sections cover the concept of privacy in VANETS; and the analysis of some existing privacy schemes. Next sections cover specific billing and incentives models and some approaches suitable for vehicular ad hoc environments. An analysis of some incentive schemes is given at the end of the section.

The second part of this thesis document introduces the proposed service architecture for spontaneous on-demand services. Chapter 4 address some key points for service provisioning and an analysis of some existing approaches related to VANETS is addressed [Coronado and Cherkaoui, 2007]. Chapter 5 covers the security model which is the foundation of the service architecture in order to provide secure session parameters [Coronado and Cherkaoui, 2007]. Chapter 6 comprises the definition of the proposed district service architecture [Coronado and Cherkaoui, 2009]. Chapter 7 details the analytical model of the scalable service architecture [Coronado and Cherkaoui, 2009]. Chapter 8 is dedicated to the study of the proposed architecture including scalable scenarios in a heterogeneous network context. Chapter 9 introduces a service taxonomy for commercial applications such as web, database, voice and video-based applications in a vehicular context and their corresponding simulation results.

Chapter 10 states the conclusions of this project as well as some perspectives on the future of the development of commercial application in VANETS.

FIRST PART

BASICS ON VEHICULAR COMMUNICATIONS

CHAPTER 2

VEHICULAR NETWORK TECHNOLOGIES

Standardization efforts for vehicular communications have been carried out primarily in North America, Europe and Japan. In North America, the DSRC technology was allocated at the 5.9 GHz frequency with a transmission range up to 1000 meters [Antipolis, 2005]. Mainly, DSRC technology is focused on safety applications and traffic information supply. These functionalities are performed through the dissemination of information for vehicles with a data rate from 6 Mbps up to 27 Mbps [Antipolis, 2005]. There are two types of messages that can be supported by DSRC, i.e. IPv6 and WSM (WAVE Short messages). The IPv6 datagrams are used to carry traffic information and requested services using a TCP/IP protocol. WSMs are dedicated to safety applications and are intended for a priority propagation among vehicles.

Based on the radio frequency specifications given in [Farradyne, 2005], channels 184 and 172 have been proposed for public safety and low latency communications, respectively. Channel 178 is the control channel establishing the communication link between the access point and the vehicle. Channel 178 can be used for communication links as well as other control and safety messages. The rest of the channels are intended for service data communications to handle IPv6 traffic. The frequency channels allocation is shown in Table 2.1.

Table 2.1 - DSRC channel allocation

5.850-5.925 (GHz)	**Channels**
172	5860
174	5870
175	5875
176	5880
178	5890
180	5900
181	5905

182	5910
184	5920

In relation with DSRC, the Vehicle Safety Communications Consortium (VSCC) [Farradyne, 2005] in the U.S. is a project aiming to analyze the requirements for vehicular safety application with an emphasis on security issues. The project considers a security model based on the IEEE P1609.2 DSRC which proposes an asymmetric cryptography to sign safety messages by frequently changing keys between two peers. This process includes the use of certificates with short lifetimes that are periodically requested by the vehicle through a nearby roadside unit.

A variant of the DSRC technology was developed in Japan. Instead, the vehicular communication takes places on the 5.8 GHz frequency. The salient applications for vehicular environments are logistics management, driver assistance, information services and electronic toll control (ETC). In particular, this technology supports different types of applications due to the implementation of the ASL (Application Sub Layer) on its architecture [Antipolis, 2005]. This is responsible for handling Internet and non-Internet services through TCP/IP or local port performing control operations over Internet connections (IPv6), local area networks and non-networks applications.

Service discovery specifications are defined in the IEEE 1609.3 [IEEE, 2003] trial standard for Wireless Access in Vehicular Environments (WAVE). Here, information related to specific providers and corresponding channels are contained in a frame called WAVE Service Advertisement (WSA) which carries the Provider Service Table (PST). Before the Roadside Unit (RSU) announces the availability of services within its transmission range, the WSA is encapsulated in an extended frame called WAVE Service Information Element (WSIE). Then, the WSIE frame is received and processed by transitory and potential users; and retrieved parameters will be employed to request specific services. The process to allow applications from a provider to be registered at the WAVE management entity (WME) consist of disclosing information such as channel of operation, address information, description of the services being offered and application priority. Once the application is successfully registered at the local PST, then it is ready to be advertised through the roadside infrastructure. In order to guarantee the certainty of the information being transmitted, the WSA frame is digitally signed and validated. In order to distinguish the different applications available at the local infrastructure, identifiers are required in the form of Provider Service Identifier (PSID) which guarantees the uniqueness of the latter. A Provider Service Context (PSC) is also used to convey additional information about the service. Based on the above process, the user can distinguish and choose specific services contained in the PST. A vehicle-infrastructure and vehicle-to-vehicle scenario is illustrated in Figure 2.1.

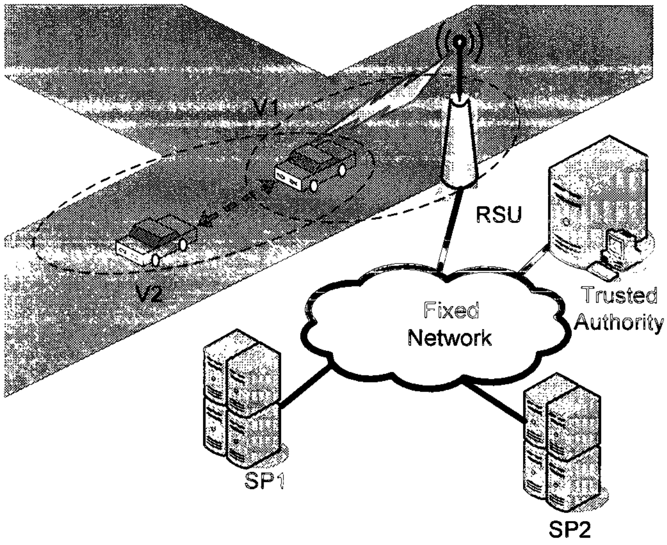

Figure 2.1 - V2V and V2I communications

2.1 Elements in Vehicle-infrastructure networks

Typical active elements involved in vehicle-infrastructure communications involving DSRC technology are briefly described according to [Farradyne, 2005] and depicted in Figure 2.2. These elements are:

The *On-board Equipment (OBE).* This equipment is installed inside the vehicle to provide communication capabilities with peers and the deployment of this electronic device depends directly on OEMs (Original Equipment Manufacturers). In general, OBEs comprise an On-

Board Unit (OBU) which is a 5.9 GHz DSRC transceiver; a GPS location system; a processor for application services; and human machine interface (HMI) to handle the interaction between the user and the services provided through communication capabilities. The communication link between the vehicle and the infrastructure in the surroundings is set up and managed by the OBU. For the transmission of safety related information, the data contained in the message includes a temporary ID, message type, time stamp and location parameters.

The *Roadside Equipment (RSE):* This equipment is the interface between vehicular peers and fixed networks. RSEs comprise a DSRC transceiver Roadside-Unit (RSU), a GPS location system, an application processor and a router that connects to the fixed network. To communicate with vehicles, the RSU transmits a list of services contained in a Provider Service Table (PST). The information transmitted includes the RSU identification, application identification, channel assignments, data rate, modulation, GPS data location and transmission power limits. Any raw information coming from an OBU is first verified in the RSU processor and then forwarded by the router to reach the network. Note that in the following chapters of this thesis document, the term RSU is used to denote the RSE.

The *Message Switch (MSW):* This element is the intelligence of the system and is located in the backbone of the network. Its main function is to handle and parse all the data intended to reach any network element. It also performs message management and subscription operations according to message priority for an efficient use of the bandwidth. The MSW will route subscribed messages to the corresponding service provider or network user. It is worth noting that all RSUs must be registered with their assigned MSW and associated to a specific region.

The *Map Server (MS):* The main function of the MS consists of maintaining the accuracy of map databases and it is logically connected to the MSW. Once an update in the position parameters has been performed in the map database, the updated information is released and sent back to the mobile peers.

Network Management (NM): The management of the network will be carried out by centralized entities known as network operation centers (NOC). These centers will be responsible for management, design, implementation, operation and maintenance of the vehicular network infrastructure.

Certification Authorities (CA): These trusted entities are responsible for dispatching secure attributes as key certificates, thus all messages passing through the network will be digitally signed.

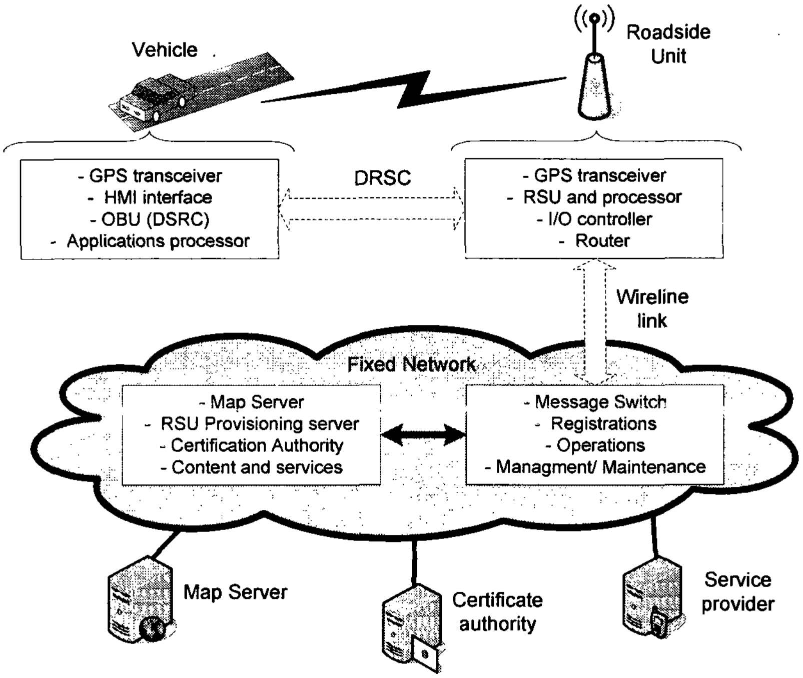

Figure 2.2 - V2I centralized architecture

2.2 Projects and initiatives

In general, initiatives that intend to provide certain level of communication capabilities to vehicles have closely collaborated with governmental authorities and the automotive industry. Most of the consortiums and initiatives have come from Europe, North America and Japan where car manufacturers are strong players in leading the integration of cutting edge technological advances within vehicles.

One example of these projects is the InternetCar which was developed in Japan. This is an extensive project which aims to support Internet applications on vehicles connected to cellular networks [Ernst *et al.*, 2003]. The addressing scheme was based on IPv6 to support IP based services offering the facilities and robustness of a highly mobile environment. Its main aim was to provide Internet connectivity to a vehicle regardless of the access medium and the applications addressed were related to the analysis and provisioning of traffic information.

An European project is FleetNet which was a three years project (2000-2003) founded by an European Consortium with the participation of OEMs and governmental institutions [Franz *et al.*, 2001]. The aim was to provide Internet connectivity on vehicles besides the propagation of safety-related applications among vehicles. The design of this solution is based on Internet gateways installed on the roadside which function as gateway routers to provide Internet connectivity. The integration of Internet applications rely on different features [Festag *et al.*, 2004]. First, a cache module allows the allocation information previously obtained from the Internet optimizing the time of distributing the information. Second, hot spot communications are intended to provide connectivity. Finally, an agent based approach which consists of a proxy server when there is no communication link between the Internet server and the vehicle. The objective is to provide certain level of coverage when there is a gap of internet connectivity mainly caused by the mobility patterns of vehicles.

The subsequent consortium created from FleetNet is the NoW (Network on Wheels) project, which deals with communication protocols for inter-vehicular communications. One of its objectives was to support safety applications as well as all sort of infotainment applications. The solution design is based on an architecture called MOCCA (Mobile Communication Architecture) [Perera *et al.*, 2005], which relies on Internet gateways posted on roadside infrastructure. These are in charge of providing an interface between the vehicles and the Internet connection with a broader scope than its predecessor the FleetNet.

Another European project is the Global System for Telematics (GST). The objective of the GST is to create an open architecture for vehicular services. The communication is done using SOAP messages and software components reside on an OSGI platform (Open Services Gateway Initiative).

Among the most popular public traffic applications, there is the ETC. The electronic payment managed by ETC is performed in a vehicular-roadside communication architecture and involves two main processes [ETC ITS, 2008]: automatic vehicle identification (AVI) and automatic vehicle classification (AVC) to perform the electronic transaction from the vehicle to the nearby fixed infrastructure. The first one (AVI) is used by the roadside infrastructure to identify the vehicle ownership based on an electronic number assigned to it. The second one (AVC) installed in the roadside infrastructure can determine the vehicle's type by its physical attributes. The deployment of ETC applications is wide. So far, Japan has the major deployment of the ETC roadside infrastructure with more than 900 tollgates [ETC ITS, 2008]. The ETC system sets the communication link between the on-board equipment and the roadside unit. In the case of Hong Kong, the ETC technology considers the use of GPS, so the vehicles equipped with GPS units communicate with the GPS satellite and are associated the corresponding toll.

In North America, specifically in New Jersey, an ETC system called E-Z was implemented on highly dense highways. The aims of this system are to mitigate congestion and save time for commuters. The deployment of E-Z has a remarkable contribution on the reduction of cost related to fuel consumptions and delay time costs.

A global integrated solution is being developed in Europe called Cooperative Vehicle-Infrastructure Systems [CVIS, 2009]. The major aims of the CVIS project consist of creating a unified technical solution to communicate vehicles and infrastructure by means of an open framework. The CVIS salient services and features are the following:

1. A multi-channel terminal capable of maintaining continuous Internet connection over different carriers, i.e. cellular, mobile Wi-Fi networks, infra-red or short-range microwave channels.

2. An open architecture connecting on-board units (OBU) and traffic management systems, as well as, roadside units (RSU). It also comprises the operation of protocols for vehicle and road monitoring.

3. Employment of dynamic mapping using GPS systems for vehicle positioning.

A Canadian initiative is represented by AUTO21 to promote research in different fields of the automotive industry such as intelligent systems and sensors; materials and manufacturing, powertrains, fuels and emissions; and design process. In the field of intelligent system and sensor applications, the following issues are targeted within Auto21 projects.

1. Vehicle guidance, navigation and telematics.

2. Control and monitoring of vehicles.

3. Driving assistance and automation.

The AUTO21 vision is stated as *"create a dynamic Canadian research and development community contributing to a sustainable, globally competitive Canadian automotive sector resulting in enhanced quality of life for Canadians"* [AUTO21, 2009].

SECOND PART

WORK AND CONTRIBUTIONS

CHAPTER 3

SUMMARY OF CONTRIBUTIONS

This chapter presents the main contributions of this work on service provisioning for vehicular environments. A secure service architecture complying with spontaneous on-demand services on the road is defined in the following chapters. These chapters, in an article based format, represent the evolution and development of this thesis project starting with the definition of security models for VANETS. The analysis of different models served to define the proposed security model for vehicular environments which is described in section 3.1. An element in the form of private authority has been introduced in the security model for the generation of security attributes to protect the delivery of the service.

A major milestone in this project is the definition of the district service architecture which is mentioned in section 3.2. In this architecture, session parameters are granted to on-demand users based upon the validation of user credentials. The service request process for a single-hop communication is given in section 3.3 on which proper validation grants the user the right to retrieve a service advertised by the roadside infrastructure. In the case where the communication requires the participation of intermediate nodes to deliver the requested service due to transmission rage constraints; then, multi-hop communication needs to be set up. This is addressed in section 3.4. In the case where mobility between adjacent district service domains occurs; then, the interaction of multiple district domains is required to maintain the ongoing service session and guarantee the scalability of the service on the road. This type of communication is described in section 3.5. Finally, different types of service applications are addressed in section 3.6, where the focus is on commercial applications and their deployment on top of the proposed service architecture.

3.1 Secure service model

In the proposed architecture, the use of pseudonyms and PKI model involves the presence and participation of both governmental and private trusted authorities. Basically, the certified keys provided by official authorities must allow secure communications between two vehicles or a vehicle and a RSU. The new element introduced is the private authority which is responsible for the generation of temporary security attributes. This feature can guarantee that heterogeneous applications from different service providers can coexist while sharing the same the roadside infrastructure. A detailed description of the security model is given in Chapter 4.

3.2 District service architecture

A service district domain is defined in this project as a logical zone that is mapped to a geographical area where a set of services from different roadside providers are broadcasted by the wireless infrastructure. The elements comprised within the service domain are in charge of processing and validating incoming requests from potential users. The service district domain may not have knowledge in advance of the prospective users. The main module elements in the scalable service architecture are described in detail in Chapter 7. A brief description is given below:

- The security module is composed of a subset of modules designated as GA and PA. Within a district domain, any disclosed public key certificate is subjected to verification. The security module generates the corresponding session keys for both the user and service provider. Moreover, a set of pseudonyms are generated which can serve as temporary identifiers for both the user and the service provider. The pseudonyms are valid only during the active service session.
- The banking module is the entity which is responsible for the issuance of on-demand credit units. These are the credentials that give the right to use a specific service. Of course, there must be a pre-established relationship between the banking entity and the user. This can be based on a special type of banking credential pre-assigned off-line. Once a successful validation is done, the banking entity is able to dispatch the

corresponding credit units and transaction identifiers which can specify the amount of content data to be retrieved or the maximum duration time for the service session.

- The session manager is responsible for establishing associations with other external session managers for the purpose of supporting scalability between multiple district domains. Any exchange of information between different district domains will be performed through the interaction of current participating session managers.
- The accounting module creates temporary registers to keep track of transitory users. These registers record the dispatched session parameters of temporary users.
- The authorization module grants resources assignation when validations at the other modules have been completed.
- The policy module defines the way the information is treated based on its labeled queuing priority and/or assigned bandwidth.

3.3 Single-hop communications

The sequence of messages and operations is described in detail in Chapter 6. This type of communication is initiated from the OBU to the neighboring RSUs. First, the OBU has to send a request message which includes its actual credentials in order to receive any specific announced service from a registered service provider. The collected information at the RSU is sent to the current district service domain where the session manager generates a session ID. In the security module, the public key certificates disclosed by the OBU need to be verified for their revocation status. If this validation succeeds, a session key and pseudonyms are generated for both OBU and the provider. In the banking module, a validation of the disclosed banking credentials and service affordability for the user is checked in order to generate the session credit units. For accounting purposes, temporary registers and associations for both the user and service provider can be created while it is authorized for that specific service session. At this point, all the parameters generated for that session are collected, protected and sent back to the corresponding recipients which are both the OBU and the provider.

3.3.1 Single-hop analysis

The analytical model for the single-hop communication scenario is given in Chapter 7 where it is defined in the single-hop initiation request protocol SHI-RQ. The cumulative signaling cost is based on the addition of individual costs at each tier process in the single-hop communication. The individual costs involve the related processing costs for performing data processing, cryptographic operations and the related link costs.

The single-hop simulation scenario is based on a user-to-district service domain tier process for processing a service request deployed in a wireless network topology as described in Chapter 8. The objective of the response time analysis is to verify its feasibility in a mobile environment when service requests are executed in a single district domain. From the results obtained, it was observed that the average response time values for the generation of service session attributes remained acceptable. These simulations were performed for a realistic number of mobile nodes and with an increased number of concurrent vehicles per access point.

3.4 Multi-hop communications

This type of communication requires some sort of incentives for participating nodes as their local resources are utilized at every received and forwarded message. Along the forwarding path, a chain of certificates must be built through public key certificates for every single intermediate node. In Figure 3.1, there are for example three intermediate nodes and the final user, in which all the nodes attach their corresponding public key certificate in the forwarding chain. At the banking entity, there is an association between an incentive unit and its corresponding public key certificate which also serves to encrypt a dispatched bonus unit and respective timestamps. Consequently, at every forwarding node, the current node will be able to decrypt its bonus unit by using the corresponding private key. The following list summarizes the steps of the above procedure of which full details can be found in Chapter 6.

1. The intermediate node attaches its public key certificate.
2. The banking module generates bonus unit and timestamp and they are encrypted with intermediate node's public key certificate.
3. At intermediate node, the received message is decrypted with the node's private key.

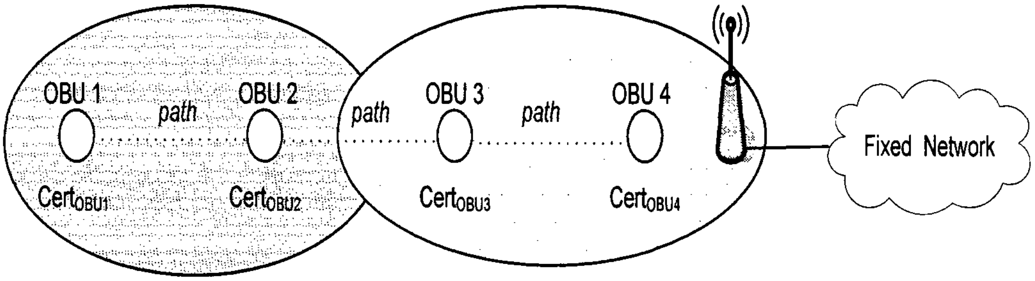

Figure 3.1 – Multi-hop communications

3.4.1 Multi-hop analysis

The analytical model of the multi-hop communication scenario is given in Chapter 7 where the multi-hop initiation request protocol (MHI-RQ) is defined. The cumulative signaling cost is based on the sum of individual cost at each tier process in the multi-hop communication. The individual costs involve the related processing costs for performing data processing, cryptographic operations and the link costs.

The multi-hop simulation scenario is based on the presence of intermediate nodes when a service request takes place as described in Chapter 6. The objective of the response time analysis is to verify its feasibility in a mobile environment when service requests are executed out of the transmission range of the roadside infrastructure. From the results obtained, it was observed that the average response time values for a service request were acceptable within a specific number of intermediate nodes. As expected when increasing the number of intermediate nodes the average response time increases as well, sometimes beyond acceptable values.

3.5 Service scalability support

In order to provide scalable solutions across multiple domains, the exchange of control messages is required between adjacent service domains so that information about active service parameters is shared among operating session managers. Interconnection mechanisms need to be established at a logical level between neighboring district domains. This is described in detail in Chapter 8. These mechanisms will allow service parameters from an active session to be shared between two concurrent district domains in order to maintain an active session alive without the need for the user to be registered for a new session at the new district domain. Additionally, scalable services between multiple district domains are likely to support the interoperations of heterogeneous access technologies

3.5.1 Scalability analysis

The analytical model for the extended connectivity request protocol EC-RQ is given in Chapter 7. The EC-RQ protocol is intended to provide as means for ensuring continuous connectivity when a vehicle changes from one district domain to an adjacent one. The exchange of current session parameters takes place when performing handover operations between different service district domains. The cumulative signaling cost is based on the sum of the individual cost at each tier process in the extended communication.

In the scalable simulation scenario described in Chapter 8, the average response time was observed to be acceptable when sharing session information even when the number of requesters increases. The response time values achieved by a single district domain are higher compared to those obtained from two and even three district domains. This is because the corresponding initial request process for a single district domain involves more tier elements and more processing to set the original session parameters.

3.6 Service Taxonomy

Different types of services are described in Chapter 9 such as safety, convenience and commercial applications. The performance of some type of applications such as HTTP, database, voice and video was studied for moving vehicles while using the mechanisms of the proposed architecture. The results collected were relative to the response time with acceptable results.

3.7 Conclusion

In this thesis project key characteristics and models for service environment in the vehicular context have been presented. The major concern is to provide a robust and secure transfer of information between a vehicles and a provider in a spontaneous on-demand manner. A scalable secure service provisioning architecture was presented, thatcomprises the presence of public and private certificate authorities collocated with accounting and banking entities interacting with active district domains. One main advantage of the district service architecture is that it promotes collaboration of the forwarding peers as the architecture generates incentives for every participating vehicle.

Three main types of request messages can take place in vehicular scenarios: a single-hop, multi-hop and a scalable service request. The simulation studies performed for single-hop, multi-hop and multiple district scenarios showed satisfactory response time values when executing service session requests.

A wide variety of heterogeneous non-safety applications can be designed on top of the district service architecture in order to offer spontaneous on-demand service access. Security of the exchanged data is preserved at all times since a service request is originated by the user till the delivery of content service from the provider.

CHAPTER 4

CONFERENCE PAPER IEEE LCN ON-MOVE 2007

This paper was presented in the IEEE ON-MOVE Workshop with the IEEE Local Communication Networks Conference (LCN) 2007, October 14-17 2007, Dublin, Ireland. The title of this paper is 'An AAA study for service provisioning in vehicular networks'. The paper gives a survey and analysis of existing approaches from an AAA perspective in mobile environments, which includes security, privacy and billing mechanisms. The concepts defined in this chapter serve as the starting point for the development of the proposed service architecture.

4.1 Abstract

4.1.1 Résumé en français

Ce document étudie les éléments clé d'une solution pour l'authentification, l'autorisation, et la facturation lors de la prestation de service dans les réseaux véhiculaires. Différentes solutions ont été étudiées pour identifier leurs avantages et inconvénients selon les paramètres principaux d'évaluation. Les efforts de recherche futurs doivent adresser ces éléments pour fournir un cadre approprié d'approvisionnement de service pour le futur déploiement des réseaux véhiculaires.

4.1.2 Abstract

This paper investigates the key elements for a scalable solution of authentication, authorization, and accounting for service delivery in vehicular networks. Different approaches

were studied to identify their advantages and disadvantages according to main evaluation parameters, two of which are scalability and latency. Upcoming research efforts need to address these elements to provide an appropriate service provisioning framework for the future deployment of vehicular networks.

4.1.3 Index terms

Vehicular networks, AAA models, service provisioning, security, privacy, billing.

4.2 Introduction

Vehicular ad hoc networks (VANETS) are networks that are enabled by short to medium-range communication systems for vehicle-vehicle or vehicle-roadside communication. The potential benefits associated to enabling road-safety applications through VANETs are well known. These include real-time collision avoidance warnings and the exchange of driving parameters among vehicles for a safer driving. Besides these useful and sometimes vital functionalities, another trend of functionalities which involves commercial non-safety related services is also envisioned by sharing the vehicle communication channel with decentralized mobile applications from different service providers. The array of these commercial services can be broad, ranging from internet access, vehicle infotainment, and navigation assistance to transportation logistics management and high speed automatic toll collection. The success of service provisioning models for VANETs for a commercial purpose depends on the implementation of robust architectures that are able to maintain their overall performance for end users when facing different real vehicular situations. In particular, new challenges arise related to security mechanisms, privacy of user information, and billing for services in a highly mobile and sometimes multi service provider (SP) context. A key point for maintaining robust service provisioning resides in the capacity to manage a series of security mechanisms which comprise authentication and authorization of subscribers. These mechanisms will provide to the involved parties a secure way to exchange information. Additionally service provider (SP) policies can regulate the provisioning of user profiles and they also can define the application of billing models. Moreover, in VANETs environments, billing processes can be extended for service message forwarding among vehicles. This can be done by the implementation of incentive and collaborative mechanisms to foster propagation of information for service delivery. This paper investigates the key elements for a scalable solution of authentication, authorization, and accounting (AAA) suitable for service delivery in VANETs.

In section 4.4, a brief description of AAA challenges involved in service provisioning for VANETs is given. In section 4.5, different existing approaches of AAA elements are presented. Section 4.6 makes an evaluation of the previous approaches based on different criteria according to VANETs characteristics and a simulation of a vehicular scenario is presented. Finally, section 4.7 presents some conclusions.

4.3 AAA challenges in VANETS

An AAA architecture is a centralized trusted model widely used by mobile network operators. A description of access models can be found in Appendix B. In this model key cryptography is built around a key management system for authentication and authorization purposes. In the case of service provisioning for VANETs, user authorization includes two levels: authorization to access a radio channel at the road unit and authorization to access a service application at the SP. Once a user has been fully authenticated, the SP grants him with the right to access services. This permission can be issued by using service credentials but SP policies can define the restrictions to access a service. Finally, a billing server infrastructure needs also to be available to charge for service usage.

In the following we will expose some specific issues that need to be addressed; primarily security, privacy, and billing mechanisms, in order to make VANETs service deployment secure for users and viable for SP.

4.4 Service concepts in VANETS environments

4.4.1 Security concepts

Security is a key point in the implementation of AAA models. It is important to keep in mind that threats in VANETs are not exclusively intended to affect vehicles; threats can also target SP. In a vehicle-vehicle communication scenario, a major concern is the injection of false information by manipulating position or speed parameters. Another well known attack is the denial of service (DoS), which can be caused by jamming the radio channel at the link layer or at the routing layer by saturating the vehicles forwarding capacity [Blum and Eskadarian, 2004]. A third attack is impersonation, where a malicious vehicle pretends to be another vehicle by forging one or more identities. Diverse types of cryptographic methods for authenticating data have been developed to secure network communications, For the purpose of this study, we briefly describe some security concepts that can be used in the VANET AAA context.

Asymmetric Cryptography. This type of authentication is based on the use of public (publicly known) and private (secret) keys for authenticating two parties. The public and the private key are mathematically related but it is nearly impossible to retrieve a private key from a public key [DoD Report, 2004]. In essence, vehicle A would have the key pairs $\{K_A, K^{-}_{\mathrm{A}}\}$ where K_A is the public key and K^{-}_{A} is the private key. To secure the communication link between vehicle A and B, vehicle A obtains vehicle *B's* public key K_B and uses it to encrypt the message. To decrypt the message vehicle B uses its private key K^{-}_{B}. The resulting security features are authentication, integrity and non-repudiation.

Symmetric Cryptography. This is considered a lightweight authentication scheme since it uses a shared secret key between two parties; thus, it is not dependant of any centralized infrastructure for key distribution and management. Basically, vehicle A and B must agree in having a secret shared key $\{K_{AB}\}$ before exchanging data and this key will be used to encrypt and decrypt messages. The resulting security features are authentication, integrity but not non-repudiation. This is because there is no trusted entity that binds the encrypted message with the corresponding real identity of the sender.

Digital signatures. Signatures provide a way to legitimize messages. They are created by encrypting the message with a private key K^{-} and decrypted by using a hash function with a public key K [DoD Report, 2004]. In the case when vehicle A wants to sign a message M, it uses its private key K^{-}_{A} to compute the digital signature as $\{M\}K^{-}_{A}$. At the receiver, the digital signature is verified by using A's public key, i.e. $\{\{M\}K^{-}_{A}\}K_{A}$. Occasionally, a collision resistant one-way hash function is applied to the message before generating the digital signature [Oppliger, 2002]. Note that the *SIG* notation is also use to represent digital signatures.

PKI (Public Key Infrastructure). This is a robust infrastructure based on asymmetric cryptography which provides generation, distribution and management of public key certificates [Mishra and Nadkarni, 2003]. The core of PKI resides in the Certification Authority (CA) who is charge of managing keying certificates. The main function of certificates is to bind the identity of an entity to a public key. For instance, the public key certificate intended to a vehicle is delivered in the form of a digital signature $SIG_{K^{-}_{CA}}(K_A)$, where K^{-}_{CA} is the private key of the corresponding certification authority (CA) and K_A is the public key of vehicle A.

4.4.2 Privacy concepts

Privacy issues for service provisioning in VANETs regard primarily preserving the anonymity of a vehicle and/or the privacy of its location.

Anonymity. It is defined as the state of a vehicle being not identifiable by any other party. Anonymity can be achieved by employing pseudonyms issued by a certificate authority which will be in charge of assigning those pseudonyms to real vehicle identities. Pseudonyms are defined as temporary identities which change over times [Capkun *et al.*, 2004]. In following sections, approaches using pseudonyms will be referred-to as time-based. In general, time-based pseudonyms provide identity privacy comprising a time metric to determine the renewal frequency of pseudonyms. The degree of privacy will be bound to the pseudonyms updating rate. (e.g. every minute). This means, that the degree of privacy increases with the updating rate. Another variant of this type of pseudonyms is what is called speed-based pseudonyms, where the pseudonyms change based on variations in the vehicle's velocity.

Location Privacy. It refers to the capability of preventing any other party to associate the vehicle's locations with its identity or pseudonyms. This type privacy is primarily intended for location based services (LBS). For instance, vehicle A located in a specific location might broadcast its information using its pseudonym; however, a third party in the surrounding can associate the user's pseudonym with its current location. To offer location privacy, schemes need to masquerade the position of the vehicle. Two examples of location privacy schemes are:

i) Mix-Zones. This scheme is intended to provide location anonymity every time an update of pseudonyms is performed in a geographic area shared by various vehicles. The changes from previous to new pseudonyms cannot be tracked due to the use of a silent period agreed on by the vehicles within the area, followed by a communication period where all vehicles change their pseudonyms at the same time; thus, causing mislead of eavesdropping activities.

ii) Geo-bound Pseudonyms. This scheme consists of assigning a set of pseudonyms according to the geographic region. This implies that the movement patterns of a vehicle will define the frequency of changes in pseudonyms, and therefore, minimizing the risk of being tracked.

4.4.3 Billing concepts

It is possible to separate billing models into two fundamental domains: *i)* A billing process that takes place at the SP infrastructure, whose main function is to charge subscribers for the use of all sorts of resources. This charging may vary depending on the SP pricing policies commonly placed in an account server. In this context, we can consider two strategies as presented in [Moustafa *et al.*, 2005]: the first one is a fixed fee, where the subscriber pays a fixed amount every period of time. The second strategy is based on charging the subscriber according to his actual consumption of resources. In general, it is worth assuming that a SP can be associated with multiple services and distributed in multiple road units. So, each service could own different access control policies and accounting schemes.

ii) The second domain is mainly oriented to ad hoc environments and deals with the presence of intermediate vehicles to reach the subscriber and the SP. In the case of VANETs, multihop approaches can be used where the participating vehicles propagate messages beyond their radio transmission range. For this purpose, incentive approaches for forwarding and collaboration must be considered as proposed in [Mohan and Joiner, 2004] and [Obreiter *et al.*, 2003] for mobile ad hoc networks. In the VANET context, the adapted schemes aiming to foster cooperation between vehicles can follow two strategies:

- ***Account based systems*** are based on the fact that intermediate vehicles in the routing path require remuneration incentives to be willing to forward other's packets. Given this condition, the participant nodes need to be aware of the neighbors' accounts or "virtual money" [Buttyan and Hubaux, 2000] to whether facilitate forwarding or drop packets. It might be considered that the issuance of accounts to vehicles is done by trusted business entities with strict remuneration policies.

- ***Reputation based systems*** are based on the trustiness of the routing path considering previous forwarding experiences with intermediate vehicles. This means, the behavior of the participating vehicles is observed and evaluated to create trusted routing paths. In general, the strategy does not consider tangible remunerations but instead it incentives collaboration by assigning reputation metrics on vehicles.

4.5 Existing approaches for VANETS

4.5.1 AAA approaches for VANETS

There has been a few works on providing AAA solution elements for VANETs. An access control scheme for application services in VANETs is proposed in [Moustafa *et al.*, 2005]. Here, the authors present an AAA framework to provide authentication and authorization based on a Kerberos model. Once a user request is released, the Kerberos Server at the SP site responds with a Ticket Grant Ticket (TGT). If succeeded, the user is eligible to be granted with a Ticket Grant Service (TGS), which manages authorization to access information services. Moreover, the authors proposed a Kerberos proxy allocated in the access point (AP or ROAD UNIT) to save bandwidth resources. After this process is complete, the user receives an IP address (IPv4) from a DHCP server and a public key certificate. With this certificate key the user will be able to authenticate other users through the generation of a pair wise master key (PMK) for mutual authentication. A major drawback is the high maintenance cost of the server infrastructure. Additionally, it is necessary to assess the end-to-end delay of the AAA process to deem its feasibility for the deployment of VANETs especially in such an extensive mobility context and dependence on internet connectivity and fast handover schemes.

4.5.2 Privacy approaches for VANETS

In [Sampigethaya *et al.*, 2005] a mix-zone location privacy scheme called Caravan is proposed. According to the authors, the main concern is to allow any vehicle to be able to achieve unlinkability between two or more of its locations while being tracked by an adversary. To achieve this, the approach combines a navigation group, i.e vehicles sharing the same geographical zone, with a random silent interval between updates of pseudonyms. Within the navigation group only one vehicle known as Group Leader (GL) is responsible for transmitting updates of pseudonyms to the group members after a silent interval. As a result, this scheme reduces the possibility to track a specific vehicle by misleading the attacker with other vehicle pseudonyms at the same time. In [Dötzer, 2005], it is addressed privacy issues in VANETs. Specifically the author assumes the use of pseudonyms as identifiers that can be mapped to identities, and that change frequently over time. The approach used to validate this scheme considers a trusted authority that is responsible of storing real identities and handling their mappings to pseudonyms. Within the vehicle, there is a tamper resistant device in the form of a smart card which stores the set of pseudonyms and credentials for accessing services. In [Raya and Hubaux, 2005] it is considered the deployment of an Electronic License Plate (EPL) as a unique identifier of the vehicle and which can be issued by a trusted authority. Regarding privacy, it is proposed the use of anonymous key pairs that change frequently according to the driving speed and can be preloaded into the vehicle Tamper Proof Device (TPD) by a certificate authority.

In summary, all the previous approaches use pseudonyms but differ in the way pseudonyms are distributed and updated, i.e. by a GL in Caravan or preloaded in a TPD.

4.5.3 Billing approaches for VANETS

There has been to date, no integrated billing approaches for VANETs that cover both their ad hoc and the infrastructure sides. Given the special characteristics imposed by VANETs, mainly on ad hoc environments, we cover in the following some relevant billing approaches in the multi-hop domain rather than billing models in a fixed network domain.

An account based approach for mobile ad hoc networks (MANETS) is presented in [Buttyan and Hubaux, 2000]. The main idea is that a node employs a currency called nugget to "pay" if it originates a request. The intermediate nodes acquire nuggets from the sent packet and then forward the later. The nugget units are distributed dynamically along the routing chain. One possible drawback of this scheme is that the number of nuggets to reach a new destination is not known in advance. In [Buttyan and Hubaux, 2003], it is proposed a counter unit called nuglet stored in a tamper resistant hardware module with cryptographic capabilities. The function of the nuglet is to count the number of originated and forwarded packets within a node. All the packets must be parsed and certified by the hardware module. If a node forwards a packet, its nuglet counter increases by one. If the node originates a packet, the nuglet decreases by one. If the counter becomes negative, the node is isolated and not allowed to originate messages. All packets must be parsed by the security model.

An alternative collaboration approach involving routing protocols for ad hoc environments is shown in [Mohan and Joiner, 2004]. There, the authors propose a model relying on a load-based routing approach to distinguish between forwarding and originating packets in the network. For route metrics, a load value takes track of the number of packets buffered per node which relates to the number of originated and forwarded packets. A node in a zone knows the topology of every neighboring node and maintains a load/hop distance table in its cache. For forwarding, the approach combines a load based hybrid routing (LHR) and a zone routing protocol (ZRP). The advantage of this scheme is that it gives a precise knowledge of the nodal activity. To stimulate cooperation the routing protocol chooses a least loaded path forcing nodes with minimum loads to forward more packets.

Based on the reputation incentive scheme, the Watchdog protocol [Obreiter *et al.*, 2003] main objective is to detect non collaborating nodes by observation and reports retrieval from other nodes. The protocol maintains a buffer of transmitted packets and observes forwarding activity of intermediate nodes by comparing each overhead packet with the packets in the buffer. If the packet has remained in the buffer longer than a defined timeout interval, the protocol marks a node as misbehaved. Furthermore, the protocol classifies routing paths according to their trustiness to avoid forwarding packets through misbehaving nodes.

Another reputation incentive scheme is the Confidant [Obreiter *et al.*, 2003] which works similarly to Watchdog in detecting malicious nodes and isolating them by using a reputation system. The scheme consists of the presence of a monitor entity which verifies that every transmitted packet by a node is forwarded by the next node. If the next node fails to forward the packet, then a warning message is released to alert about the corresponding malicious node. Subsequently, the system builds a routing path by ranking the nodes and removing the paths containing malicious nodes. The difference with Watchdog stands in the fact that Confidant excludes misbehaving nodes from routing paths.

From the works presented above, and given proven billing models for wireless infrastructure-based networks not presented here, one can see that a remaining open issue in billing models for VANETs relies in the integration of billing mechanisms that can be implemented seamlessly both at the infrastructure and at the ad hoc network, and that can be easily operated at the SP. The challenge relies in that the billing process performed on the accounting server at the SP site, needs also to be aware of the forwarding transactions carried out by the vehicles. This can be thought of in terms of a billing hybrid scheme for VANETs.

4.5.4 Security approaches for VANETS

There have been different proposals for securing data in vehicular environments. In [El Zarki *et al.*, 2002] a Driver Ad Hoc Networking Infrastructure (DAHNI) is proposed. The authors assume vehicular ad hoc networking with access to a fixed infrastructure and which is intended mainly for traffic management. For security the authors implement digital signatures based on RSA (Rivest Sharmir Algorithm) encryption. These digital signatures are issued along with timestamps and sequence numbers to provide authentication between two parties. For managing public keys, a PKI infrastructure is envisioned adding robustness to the system.

In [Raya and Hubaux, 2005], it is addressed the challenges of implementing security in VANETs. Similarly to [Raya *et al.*, 2006], the security architecture is composed by a Vehicular Public Key Infrastructure (VPKI), where a CA issues certified public/private key pairs to vehicles. Authors also consider a hardware device tamper proof (TPD) to keep keying materials. In the authentication procedure, the vehicle signs each message with its private key and attaches the corresponding public key certificate. For digital signatures, the encryption method is ECC (Ellyptic Curve Crytographic) with a significant reduction on the packet size.

In [Blum and Eskandarian, 2004], it is described the threats on inter-vehicular communications and present their project called SecCar. They assume a PKI architecture and a virtual infrastructure formed by cluster heads. The later are responsible for signing messages and disseminating them via a unicast transmission. A limitation of this approach is that it can create a bottleneck when traffic increases. It also increases the packet overhead.

Besides the research works mentioned above, in [Choi *et al.*, 2005] a different perspective on securing VANETs is presented. The work states a model that supports a symmetric scheme over hybrid architectures without the need of a centralized infrastructure. The authentication between vehicles and base stations (BS) is performed through a message authentication code (HMAC), which is a cryptographic hash function that uses a symmetric key. The HMAC verification is done with the shared session keys which are computed by the vehicles and the BS using pre-shared long lived pseudonyms. According to this proposal, the non-repudiation feature can be achieved by means of a trusted entity (most of the time off-line) which is responsible of providing a link between an identity and a corresponding pseudonym.

In summary, it is possible to classify security approaches existing in current works into two broad branches, i.e. symmetric and asymmetric mechanisms implemented within a PKI infrastructure, where repudiation is assured by asymmetric mechanisms.

4.6 Evaluation of existing approaches

In this section, we present a qualitative evaluation as well as some quantitative evaluation measures for the different AAA element approaches presented earlier. Similar to [Fonseca and Festag, 2006], we evaluate the approaches described in the previous sections as having good, average or poor performance for a number of criteria. The following criteria have been examined for all categories of AAA elements: scalability, packet overhead, latency, and processing.

Scalability: it is related to the level of network performance as the number of vehicles increases. Three levels of scalability can be noted good (large networks), average (medium size) and low (small networks).

Adaptability: it refers to the way the network topology converges to changes in its topology. The difference with scalability is that the latter refers to the capacity to extent services and support a large number of users.

Packet Overhead: it deals with the additional data that is appended to the message to provide the particular element of AAA. Three levels of packet overhead where considered.

Processing: it refers to the computational resources required for the computing and processing related to an AAA element. Three levels of processing requirements where considered.

Latency: It comprises the total time delay of message or data generation and/or propagation and/or processing involved in the logical operation of a particular AAA element. This parameter can be directly related to the processing and packet overhead criteria. If the processing and/or packet overhead increase, the expected latency will increase as well. The latency has a direct impact on the degree of feasibility or adequacy of an AAA element in the VANET context. The higher the latency, the bigger the requirements on the performances of handover and mobility management mechanism on the networking level for VANETs.

4.6.1 Analysis for security approaches

In addition to the evaluation criteria mentioned above, we also consider here the adaptability. The latter refers to the ability of the approach to handle and support frequent changes in the VANET topology especially. Note that this criterion is related to the scalability of the network. The level of adaptability can be good (support frequent changes), average (medium support) and low (minimum support).

Table 4.1 shows a comparison among symmetric, asymmetric and digital signatures schemes.

Table 4.1 Comparison of security schemes

	Symmetric	**Asymmetric**	**Signatures**
Scalabiltiy	Average	High	High
Packet OH	Low	Average	High
Processing	Low	High	High
Latency	Low	High	High
Adaptability	Average	High	High

As shown in Table 4.1, symmetric algorithms have average scalability since a secret key must be shared between two parties. Complexity increases as the number of vehicles increases, since new shared keys need to be created for every incoming vehicle. Symmetric schemes have, however, low processing requirements since unique secret keys are already known by the parties; thus, the packet overhead is also low independently of the selected encryption mechanism. For example, HMAC using a symmetric key can be generated by a SHA-1 hash function, which is 20 bytes long. The main advantage of symmetric algorithms is that exchange of information can be performed in short periods of time; as a result, one can assume that end to end latency is low which is desirable in such highly mobile environment. Note that, symmetric schemes offer authentication and integrity protection to data but they do not assure non-repudiation. For example, when law requisites need to identify and punish misbehaving activities. But as described in [Choi *et al.*, 2005] it is possible to retrieve identities from a trusted entity built around a symmetric scheme.

In the case of asymmetric schemes in PKI, they pose good scalability and adaptability to frequent changes in extended VANETs since the distribution of key pairs and certificates is performed by a centralized entity. In contrast, the main disadvantage is the high processing requirements which suggest an implicit increase in the end-to-end delay. Regarding the packet overhead, it is considered average since no additional signaling packets are required along with the message. It is worth noting that digital signatures use asymmetric mechanisms, thus, scalability and adaptability to frequent changes remains good as long as the mechanisms use a centralized key distribution. Regarding the packet overhead, it increases due to the signing and verification process for every transmitted message. This also has a negative impact in the computational processing. Nevertheless, as proposed in [Mohan and Joiner, 2004], processing problems can be alleviated by using specific hardware devices in charge of storing keying material and signing messages. Moreover, as explained in [Fonseca and Festag, 2006], power constraints due to high processing requirements are not a concern in VANETs since vehicles are equipped with long life batteries.

In the following, we analyze through simulations the effects of packets size when using digitals signature on the overall round-trip delay. We consider a request-reply registration scenario where a requester sends signed registration messages to a nearby road unit (RU) in order to assess the impact of the message round-trip delay (RTD) [Raya *et al.*, 2006]. This RTD is given by,

$$T_{RTD(M)} = 2*(T_{sign(M)} + T_{Tx(M)} + T_{verify(M)}) \qquad (1)$$

where $T_{RTD(M)}$ represents the round-trip delay for a registration message M. This involves that a registration request messages is attached with the vehicle's signature and on the other side the RU also signs the reply messages. $T_{sign(M)}$ is the time to generate a signature of message M, $T_{Tx(M)}$ and $T_{verify(M)}$ is the time to transmit and verify message M, respectively. It is possible to approximate the processing time for an ECDSA signature such as given in [Raya *et al.*, 2006]. Notice that there is no handshaking in the previous formula; it only represents the round trip delay. The time values for this signature are given in Table 4.2.

Table 4.2 Signature Processing times

Operation	**Time(ms)**
Generation	3.255
Verification	7.617
Transmission	0.110

Simulations were implemented in NS-2 simulator using MAC 802.11a module with a data rate of 54 Mbps. We evaluated the round-trip delay at different vehicular speeds and different packet size.

Figure 4.1 shows the number of packets received at different speeds considering registration messages of 256 bytes with a periodicity of 100 ms. As can be seen, the lowest amount of 21 packets received is reached at 50 m/s. It can be inferred that as long as the vehicle is moving at high speeds, the periodicity of the registration messages should be increased since the vehicle approaches rapidly the boundaries of the radio transmission range. The maximum distance achieved between the RU and vehicle was 550 m and beyond this distance no request-reply messages were received.

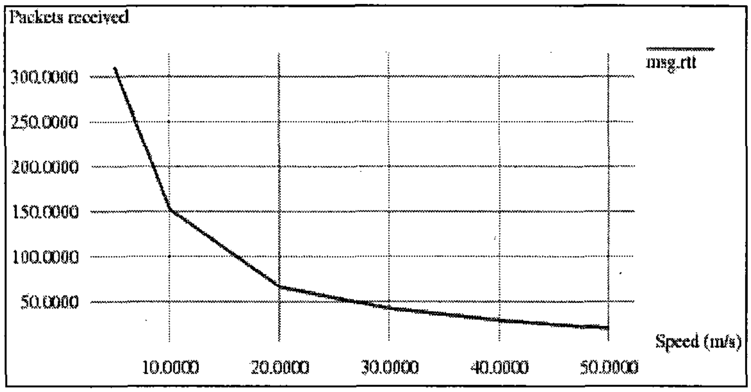

Figure 4.1 - Received packets vs speed

Figure 4.2 shows the round trip delay at 10 m/s (continuous line) and 40 m/s (dash line) speeds with a registration message of 256 bytes and a periodicity of 50 ms within a 5 s transmission window time. As shown in the graph, the round-trip delay at 10 m/s presents several delay peaks due to farther positions from the RU at that transmission time window compared to a vehicle moving at a 40 m/s.

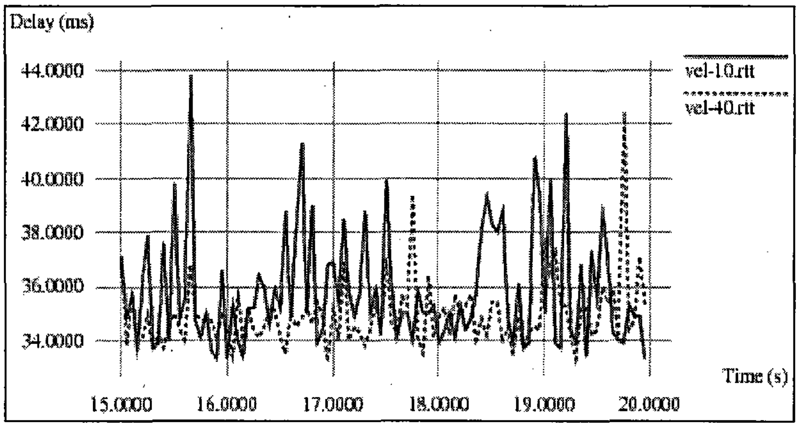

Figure 4.2 - Round trip delay vs time

4.6.2 Analysis for privacy approaches

In addition to the general evaluation criteria mentioned above, we also consider here the unlinkability. It refers to the property of not being identifiable from the previous to the current position. The level of unlinkability is considered to be high, average and low. Packet overhead depends on the additional data appended to the message to provide privacy attributes and latency comprises the additional time delay caused by the generation of privacy attributes.

Table 4.3 - Comparison of privacy schemes

Metrics	Time-based	Mix-zones	Geo-bound
Scalability	High	Average	Average
Overhead	Low	High	High
Processing	Low	Average	Average
Latency	Low	High	Average
Unlikability	Low	High	Average

As shown in the Table 4.3, the time-based privacy presents high scalability features due to every vehicle generates its own pseudonyms independently from any third trusted entity or any delimited geographic area. The corresponding packet overhead deals basically with the type of cryptographic key used to generate the pseudonym. A common cryptographic scheme is HMAC with a fix length of 160 bits using SHA-1 [Capkun *et al.,* 2004] and consequently the processing requirement is low. The communication transmission does not have a relevant latency impact if the generation of pseudonyms for a specific vehicle uses fast encryption schemes, e.g. MD5 or SHA-1. Moreover, the renewal of pseudonyms can be predefined depending on time or speed parameters. Regarding unlinkability, time-based approaches are oriented to provide identity anonymity and they are not intended to support location anonymity.

The mix-zone approach presents average scalability features since it is oriented for a delimited area with a registration control for the members of a secure area. The overhead and latency are considerably high especially if the registration access to the area is configured in a cluster mode, where control mechanisms relies on a vehicle supervisor entitled to control and distribute pseudonyms. This configuration can cause a severe bottleneck effect if the number of node member increases. Unlinkability is the salient feature since multiple pseudonyms will be transmitted in the zone simultaneously with no possibility to correlate the current position and numerous pseudonyms for a specific vehicle.

The geobound scheme assigns a predetermined set of pseudonyms to a specific geographic zone. Similar to the mix-zone approach, there is a registration and access control performed by a principal entity in the corresponding area in order for the vehicle to retrieve local pseudonyms. Therefore, there is an average scalability since every zone distributes and monitors its pseudonyms in the bordered area. The packet overhead will have a significant impact when the vehicle changes from one zone to and adjacent zone. This implies a registration process in the new zone to receive the related pseudonyms. Latency is considered average since once the vehicle is registered in the zone there is a direct distribution of pseudonyms. Even though, pseudonyms change depending on the geographic zone, unlinkability is not fully assured if the pseudonyms are being tracked by a third party from a zone to another. From the above discussion, one might think that time based approaches best suit the characteristics of VANETs but their major drawback is that location anonymity is not guaranteed. In some vehicular scenarios, a combination of time based and location base privacy approaches might be required, so further analysis must to be done on this subject.

4.6.3 Analysis for billing approaches

We compare reputation systems in the form of the Watchdog and Confidant approaches and account schemes in the form of load based and credit based approaches. Scalability of billing approaches is related to the capability of the incentive approach to handle large size network. Packet overhead is related to the additional data appended to the message to assure cooperation between vehicles. Latency comprises the additional time delay caused by the implementation of incentive approaches. Additionally, we consider the negotiation criterion which refers to the capability of a vehicle to negotiate incentive units with an authorized entity. In general reputation schemes do not support this feature.

Table 4.4 - Comparison of incentives schemes

Metrics	Watchdog	Confidant	Load-based	Credit
Scalability	Average	Average	Average	High
Overhead	Average	Average	High	Average
Processing	Low	Average	High	High
Latency	Low	Average	Low	Average
Negotiation	No	No	No	Yes

As seen from Table 4.4, the Watchdog scheme holds an average scalability capacity since each vehicle must keep a trustiness metric and knowledge from all the vehicles in the forwarding chain. A possible limitation appears if the routing path extends. There is an average packet overhead caused by the report of vehicles and observation of the forwarded packet in the routing chain. Moreover, the routing metric calculation and buffering of the packet overhead is carried out by each vehicle after transmitting a packet. This means, that the reputation actions come after the routing event, i.e. detection of abnormal behavior, and consequently with no relevant impact the overall latency. As mentioned in section 4, this is a reputation based incentive scheme intended to operate in the network layer with no negotiation capabilities.

Confidant has an average scalability especially when the number of vehicles increases due to the maintenance of the routing tables after the reputation system has ranked every vehicle in a routing path. Consequently, there is a significant impact on the packet overhead and processing when the alarm message is triggered to alert trusted vehicle from malicious nodes. Routing paths have to be reordered and ranked affecting the overall latency. Similar to Watchdog, this is a reputation based incentive scheme intended for the network layer with no negotiation capabilities.

The hybrid load based routing protocols presents an average scalability since every vehicle in a specific zone knows the topology of the neighboring vehicles within the zone. Problems will rise up if the number of vehicles increases. To control the access of vehicles in the zone, access protocols have a big impact on processing and packet overhead. Regarding latency, the packet will follow the least load routing path within the zone assuring a minimum end-to-end delay. In this scheme no negation is available since it uses a load metric based on the number of packets to define routing paths within the zone.

Account based approaches, as nuggets or nuglets schemes provide good scalability since every vehicle manages its own counter independently of any exchange of routing tables from neighboring vehicles. The main assumption is that counter units cannot be modified by the users due to the existence of tamper resistant hardware [Buttyan and Hubaux, 2005]. Since every packet needs to pass through the secure hardware it verifies and inserts the encrypted current counter in the packet header causing an increase in overhead and processing requirements. This implies also a significant impact on the overall latency. The main advantage is that this approach support negotiation between the vehicle and the account entity responsible of assigning counter units; thus, flexible remuneration can be established for specific network connections.

Considering a business perspective in VANETs, the account based approaches are more likely to meet the characteristics of dynamic billing applicable in ad hoc environments.

4.7 Conclusions

This work presented an AAA study focused on service provisioning in VANETs. Security is an element that is central to AAA approaches. Two major categories of security mechanisms are researched in current works, i.e. symmetric and asymmetric schemes. Based on the latter, a PKI infrastructure with digital signatures can be implemented offering a robust secure scheme. PKI has some significant drawbacks in the context of VANETs such as a high processing requirement and consequently an increase in the end to end latency. However, major benefits can be outlined from this scheme considering the potential deployment of road access infrastructures with the approval and support of governmental authorities.

Regarding privacy issues, these are interested in preserving identity or location anonymity. For the latter, mix zones and geobound schemes were analyzed while time based pseudonyms were considered to provide identity privacy. In some vehicular scenarios, a combination of time based and location base privacy approaches might be required, so further analysis must be done on this subject.

One major issue when implementing billing models for VANETs is the integration of robust billing mechanisms that can be implemented at the infrastructure and at the ad hoc level of VANETs and be operated seamlessly at the SP. The resulting model may need to provide incentives to vehicles to foster collaboration between them. In ad hoc environments, the account based approaches are more likely to meet the characteristics of dynamic billing in VANETs. The following chapter covers the security model which is the foundation of the service architecture in order to provide secure session parameters [Coronado and Cherkaoui, 2007].

CHAPTER 5

CONFERENCE PAPER ITS-UBIROADS IN IEEE GIIS 2007

This chapter presents the paper published at the International Workshop for Intelligent Transport Systems ITS UBIROADS, co-located with IEEE Global Information Infrastructure Symposium GIIS, July 2-4 2007 in Marrakesh, Morocco. The title of this paper is 'Secure Services in Vehicular Networks'. This chapter defines a secure model suitable to maintain secure communications in a vehicular environment. This secure model definition will serve to define an extended service architecture to provide on-demand services on the road.

5.1 Abstract

5.1.1 Résumé en français

Le succès des déploiements courants d'une série de services pour les conducteurs et les passagers permet d'envisager un futur prometteur pour les services basés sur les réseaux véhiculaires. Des architectures sécurisées remplissant des conditions de mobilité véhiculaires doivent être conçues afin d'offrir les communications fiables sur lesquelles ces services peuvent être déployés. À cette fin, une architecture comprenant les entités gouvernementales et privées est présentée en ce document. Des scénarios sécurisés d'approvisionnement de service sont illustrés et donnent une vue d'ensemble sur la façon dont des mécanismes sécurisés peuvent être mis en œuvre application pendant les sessions de service demandés par les véhicules.

5.1.2 Abstract

The current deployment of a variety of services for drivers and passengers envisions a promising future for vehicular networks (VN). Secure architectures fulfilling VN

requirements must be designed in order to offer reliable communications on top of which these services can be deployed. For this purpose, a trusted authority architecture including governmental and private entities is presented in this paper. Furthermore, secure service provisioning scenarios are illustrated giving a broad view on how secure mechanisms can be implemented during service sessions.

5.1.3 Index terms

Vehicular networks, service provisioning, security.

5.2 Introduction

Nowadays, current research works dealing with diverse aspects of vehicular networks (VN) are carried out by automotive industry in conjunction with some governmental entities and academic entities. Some of the initial efforts in this field began with the development and standardization of vehicular communication technologies. That is the case of DSRC in North America and Japan, as well as some European projects such as FleetNet [Hartenstein *et al.*, 2001], and NoW (Network on Wheels) [Gerlach, 2005]. One of the main objectives of these technologies is to enable precaution information to drivers in the aim to reduce the number of traffic accidents. For instance, DSRC communication capabilities will allow the broadcast of safety messages between vehicles in the proximity of an unsafe area to alert drivers of imminent dangers on the road, and allowing them to take preventive actions with sufficient time to avoid accidents. The deployment of such technologies originally intended for critical applications, also opened the opportunity to provide a vast variety of other business driven applications. Examples on this realm include driver assistance navigation, road information services, and infotainment services for passengers (e.g. games, file downloads, video on demand, Internet connectivity). Even though, some of these applications may have real-time constraints, they encompass different requirements and characteristics compared to those concerning safety applications. For example, service delivery is usually targeted to a specific vehicle or passenger, but communication technologies would broadcast the requested service within the limits of the radio transmission range. As a result, this introduces new challenges in vehicles and users authentication. Also, service delivery might involve forwarding and propagating data in an ad hoc mode beyond the communication range of an access point. Vehicles forwarding data might behave in a malicious way based on the premise that neighbouring vehicles are considered to be untrusted entities by nature. In this context, new challenges arise to support reliable transfers of information among unknown vehicles and service providers (SP). In general, it is required that future vehicular service systems guarantee the availability, reliability of services, as well as, security and privacy of users. Secure architectures fulfilling VN requirements must be designed in order to offer reliable communications on top of which vehicular services can be deployed.

In this paper we introduce a trusted authority architecture which comprises the collaboration of governmental and private entities. Secure service provisioning scenarios are also illustrated giving a broad view on how secure mechanisms are used during service sessions. In section 5.3, we give a brief description of the main communication elements directly involved in the architecture proposed in this paper. In section 5.4, we present the proposed security model and describe the main function and its elements in typical single hop and multi hop scenarios in section 5.5. Finally, some discussion in section 5.6 and conclusions in section 5.7.

5.3 Secure service provisioning architecture

Most of the secure models rely on a Certification Authority (CA) which is responsible of distributing and managing certified cryptographic keys between communicating parties. CAs are also responsible of keeping control of records and identification of vehicles. In our proposed architecture, we rely on the use of pseudonyms and a PKI model involving both governmental authorities and private trusted authorities.

5.3.1 Governmental trusted authorities (GA)

It is possible to consider the type of key provisioning by *GA* as permanent or semi-permanent depending on governmental policies and regulations. This control might allow an official authority to identify the real identity of vehicles under certain legal situations. In [Raya and Hubaux, 2005], it is proposed that regional governmental authorities and possibly car manufacturers could be in charge of these operations. Once the security material is available, it is preloaded in tamper-proof devices within the vehicle.

In essence, the certified keys provided by *GAs* must allow secure communications between two vehicles or a vehicle and a RSU, even if no previous communication between them has been set up. This principle is supported by the assumption of the execution of strict control and registration procedures applied to all vehicles and RSUs within the fixed infrastructure.

5.3.2 Private trusted authorities (PA)

In the proposed architecture, *PA* may also be involved in a certification process. Based on a business premise, we might think in terms of fixed infrastructures which involve the partaking of heterogeneous applications from different service providers. For this reason, it is not suitable to consider the set of pseudonyms and key certificates associated to a vehicle to be preloaded in advance before contacting a specific SP. Such a scenario would in fact mean that a user must previously store the public key for every SP he would like to contact and also its corresponding set of pseudonyms. In our architecture, *PA* represents certified companies in charge of providing pseudonyms, key distribution and key management for on-demand requesters, i.e. users and SPs. The difference between *GA* and *PA* relies in that the latter issues temporary key certificates and pseudonyms valid only during the service session. This means, every time a user requests access to a service, a new pseudonym and key certificates are assigned for that specific session. Certainly, active collaboration between the *GA* and *PA* legitimate all communicating parties.

The elements involved in the proposed architecture are presented in Figure 5.1. These elements can be used both in a compulsory service subscription scheme and in a temporary service registration scheme. In the first scheme, the user is required to register previously in the SP's records in an off-line process and be submitted to an authentication and access control procedure performed in the SP's domain during an on-line process. In the second scheme, no previous subscription is needed. This is the case, for example, when a SP advertises on-demand services through the roadside infrastructure, however, the exchange of this type of information must also be secured. It is worth noting, that we assume a previous trust relationship between the SP and RSU, since the MSW must contain accurate and reliable information of available SPs.

The operation of the architecture and its elements is illustrated in two typical scenarios of single-hop and multi-hop service provisioning.

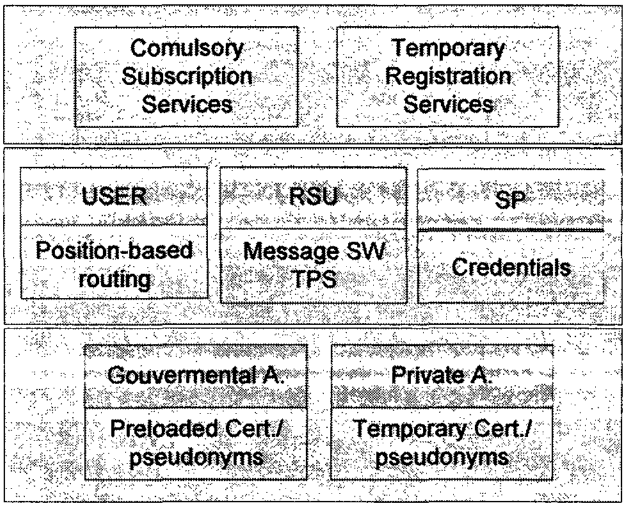
Comulsory Subscription Services
Temporary Registration Services
USER
Position-based routing
RSU
Message SW TPS
SP
Credentials
Gouvermental A.
Preloaded Cert./ pseudonyms
Private A.
Temporary Cert./ pseudonyms

Figure 5.1- Secure service architectural elements

5.4 Single-hop service provisioning

This might be the typical case of a service provisioning scenario where the vehicle has relatively slow mobility or stays immobile before a nearby RSU infrastructure; thus, it can be inferred that the service session can be established within the radio transmission range. In a subscription scheme, one might think that most of the SPs would require detailed user information for contract procedures, but for operation purposes real user information must not be disclosed to any other party. Therefore, the employment of pseudonyms can guarantee user privacy from eavesdropping activities in the surroundings.

As discussed earlier, preloaded key certificates and pseudonyms are provided by *GA* and must allow any vehicle to establish a secure communication with its peers. This can also be extended to the communication between the vehicle and the RSU. On the other hand, the generation of temporary pseudonyms and key certificates for service sessions must be taken by *PA*. Figure 5.2 illustrates a general single hop scenario.

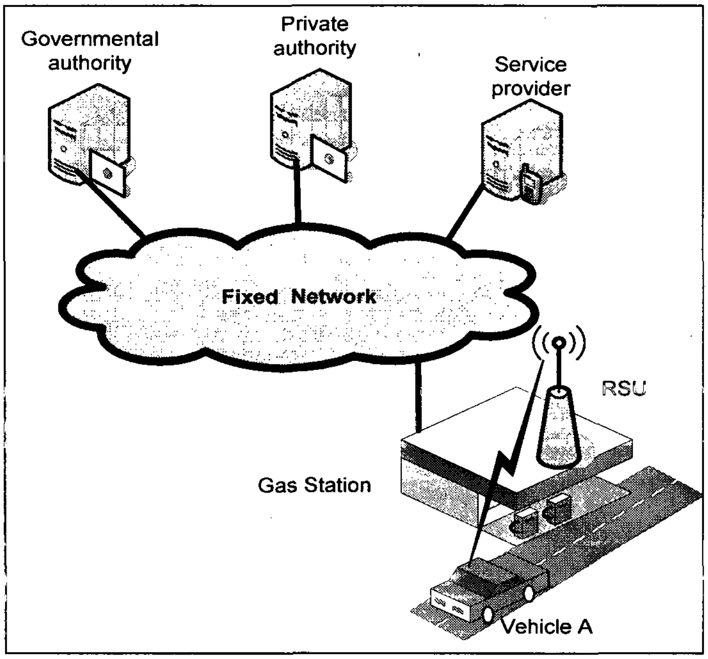

Figure 5.2 - Single-hop scenario

As mentioned in the previous section, the RSU is logically connected to the MSW and this latter provides a Provider Service Table (PST) containing a list of service identifiers, addresses and detailed data from all the SPs registered in that specific RSU. For the analysis of this scenario, assume that a potential user obtains the PST information which was broadcasted by RSU *A* within the transmission area. At this moment, the user might know the type of service that he is willing to request.

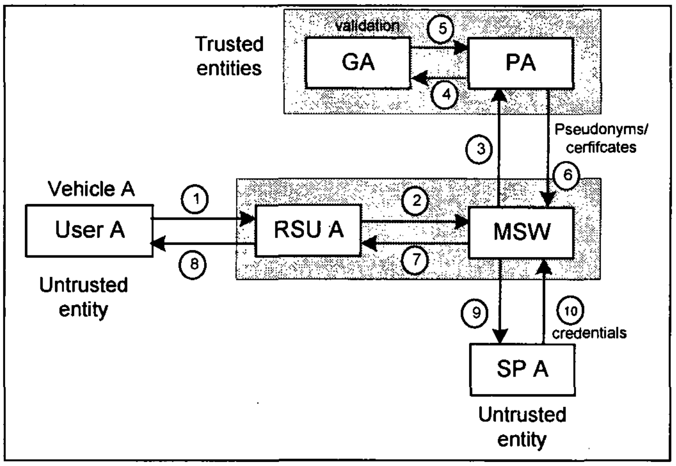

Figure 5.3 - Single hop registration diagram

Figure 5.3 show the registration diagram in a single hop scenario. Initially in step 1, user *A* transmits a signed service request message to RSU *A* containing its preloaded pseudonym, current time and service identifier retrieved from the PST list. At the RSU, the signed message request is verified and then passed to the MSW in step 2. At the MSW, the user's service request is parsed and the service identifier is matched with a specific SP name and IP address, as well as the *PA's* IP address. In step 3, a secure-attributes request message containing the preloaded user's pseudonym is forwarded from the MSW to the *PA*. Once the *PA* receives the request message, the certainty of the preloaded pseudonym needs to be verified by the *GA* by sending a validation request message in steps 4-5. Forged pseudonyms can be detected since the *GA* is responsible of issuing official security attributes for all vehicles. As soon as the validation is retrieved, in step 6 the *PA* is able to generate and forward to the MSW both a temporary pseudonym and key certificates. The resulting signed reply message intended for the user is then transmitted via the RSU in steps 7 to 8. Subsequently, in step 9 the *PA* generates both temporary pseudonym and key certificates for the SP via the MSW in the same way as it was done for the user.

Once, temporary pseudonyms and key certificates are available at both ends; the user can transmit a signed session request message containing its username and password to be validated by the SP databases in the case of a subscription-based scheme. Pseudonyms are dispatched along with the session parameters and encrypted by the user's public key. Then the user can use its pseudonym when retrieving the service. Additionally, pseudonyms might be traceable by the district domain. At this point, the SP will be able to authorize or reject the session request message based on the user's profile and/or SP's policies. Note that in the case of temporary registration scheme, the SP creates temporary registers in its databases for that specific user, thus there is no need to assign the user with a permanent username or password. If the session request is authorized, the SP generates a set of credentials exclusive only for the service session (step 10), thus credentials will expire after its use. In general, all the information is secured by signing and verifying messages through the entire path from the user to the SP.

Moreover, to minimize the risk of eavesdropping activities that correlate the temporary pseudonyms with actual user identities by malicious parties, it is possible to consider changes of pseudonyms on a time-based expiration scheme during the service session. That means that the user will need to request a new set of secure attributes to the *PA* when the current ones have already expired.

In general on this provisioning model, authentication, integrity and non repudiation requirements are guaranteed at each connection point.

5.5 Multi-hop service provisioning

In this scenario, there are two communication approaches to consider; one related to ad hoc dissemination among vehicles, mostly consisting of position-based routing protocols (e.g. geocast addressing); and the second one is a forwarding scheme comprising topology-based routing protocols, as commonly used in fixed networks. On the ad hoc side, it is assumed that vehicles are able to communicate each other through wireless technology within a certain transmission range (up to 1 km for DSRC for example). Furthermore, vehicles are most likely able to determine their position parameters and also the position to the closest RSU when this is beyond the radio transmission range. This can be possible since it is expected that the vehicles adapted for VN and RSUs will include positioning systems devices such as GPS transceivers as explained in the previous section. A general ad hoc to infrastructure communication scenario is shown in Figure 5.4.

For the ad hoc domain, a secure position-based ad hoc routing means to include the vehicle's position coordinates within the addressing parameters used to forward messages to their corresponding geographical destinations. Here, the original message is signed by the sender's private key including its position coordinates, certificate and a timestamp. Then, the intermediate vehicle validates the previous vehicle' signature, removes the certificate and records the position of the previous vehicle. This is to verify the authenticity of the previous vehicle. Then it attaches its own signature and certificate and forwards the new message to the following intermediate vehicle and so on until the messages reaches the final destination. It is worth reminding that initial secure attributes provided by *GA*s must allow any vehicle to establish a secure communication with its peers. As seen in Figure 5.5, the protocol is similar to the one explained in the single hop scenario. The main difference between both diagrams stands in the ad hoc part.

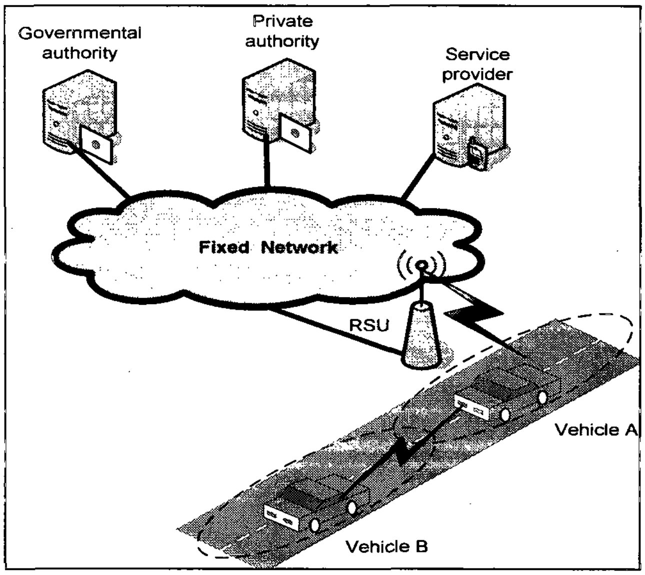

Figure 5.4 - Multi-hop scenario

For the analysis of this scenario, assume that a potential user obtains the PST information from the RSU and which was propagated beyond the radio transmission area. Initially, user *B* forwards a signed service request message to the user *A* as shown in step 1. The parameters contained on the messages comprise the preloaded pseudonym, position coordinates, certificate, service identifier obtained from the PST list and the RSU's position.

When the message arrives to user *A*, the signature from user *B* is verified and the certificate is removed. After this is done, user *A* signs the message and appends its own certificate. In steps 2-3, the signed message passes to the MSW via the RSU. At the MSW, the information from user *B* is retrieved and parsed to be processed. In step 4, a secure attribute request message is sent to the *PA* regarding the information of user *B*. At this point, the *PA* contacts the *GA* in order to verify the virtual certainty of the current pseudonym of user *B*. Once this is done, the *PA* is able to generate the correspondent temporary pseudonyms and key certificate for user *B* (steps 5-7).

After this, a reply message which includes a temporary pseudonym and key certificates are forwarded back to vehicle *B* following the same route as the initial request message (steps 8-10). Consequently, the *PA* provides the secure attributes to the SP via the MSW in step 11.

Now, both user *B* and the SP have acquired the secure mechanisms to exchange information from the ad hoc side till the fixed network. Therefore, user *B* can send an access request message intended to reach the SP and which contains its username and password. When the SP receives this message, the SP can grant or refuse the provision of credentials depending on its business policies and user profile. If authorized, the SP replies to the user a signed message including the service credential and a certificate. The route backwards follows the same route as in the initial forwarding. It is worth noting that the certificate appended by the SP is the one issued by the *PA*, while the certificates appended by the intermediate vehicles are issued by the *GA*. Note that this study does not consider major drawback effects regarding mobility issues as high speed mobility, multipath signal propagation or handovers schemes.

In summary, the exchange of service messages is secured by adding signatures on each forwarding point. This procedure can guarantee that the message is legitimated by the participating intermediate vehicles along the route from the user to the SP. One should keep in mind that this condition can be accomplished only if there is a collaborative behaviour between vehicles; otherwise, the implementation of individual incentives might be required to foster their cooperation.

5.6 Discussion

As can be noticed from these scenarios, one limitation of the previous models deals with the packet size and processing overheads since every message needs to be signed and verified at every forwarding point. This can become a significant issue especially for the ad hoc scenario if the number of intermediate vehicles to reach the destination increases. On the other hand, the advantage of implementing robust security schemes based on PKI becomes evident. This means that integrity, authentication and non-repudiation features of data are guaranteed by the use of digital signatures which in fact relies on the validation of not only one but two trusted authorities.

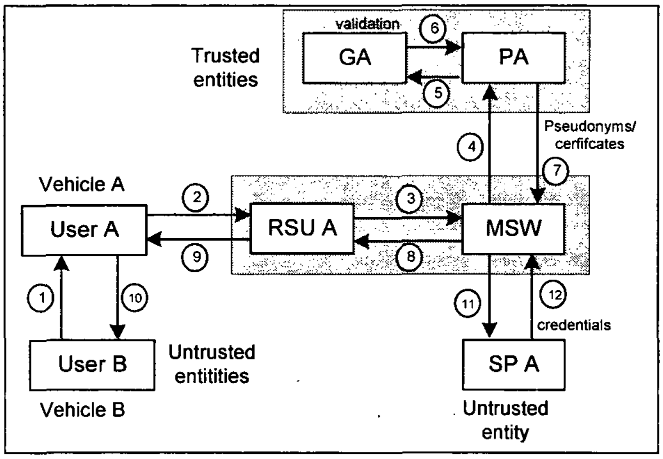

Figure 5.5 - Multi-hop registration diagram

In addition, the use of temporary pseudonyms increases the protection against possible privacy attacks; nevertheless, location privacy cannot be provided, especially in the multihop scheme, since the delivery of services depends on position based routing protocols for message forwarding. Further simulation analysis concerning the evaluation of the overall performance needs to be performed. Also, the analysis of location privacy techniques must be considered when service provisioning takes place on dynamic vehicular ad hoc networks.

5.7 Conclusions

One major concern for service provisioning in VN is to provide a robust and secure transfer of information between the user and the SP. Based on the premise that neighbouring vehicles are not trusted entities, as well as SP's, the presence of trusted authorities is required to provide security attributes to communications. The trusted authorities considered in this work can be classified into governmental and private entities. The first ones, as public bodies, keep strict control of vehicle records and provide certificates to vehicles. The second entities provide temporary pseudonyms and certificates to parties under on-demand service situations. The interaction between both trusted entities guarantees the legitimization of the communicating parties. Delivery of services might be performed in a single-hop or a mutli-hop to reach the fixed infrastructure. In both delivery scenarios, the right to access a service is issued by the SP in the form of credentials associated and valid for a specific service session. There are still some open issues to be considered, one of them is location privacy in secure delivery models.

The following chapter comprises the definition of the proposed district service architecture based architectural elements to offer spontaneous on-demand service on the road. [Coronado and Cherkaoui, 2009].

CHAPTER 6

JOURNAL OF AUTONOMOUS AND ADAPTIVE COMMUNICATIONS SYSTEMS – IJAACS 2009

This chapter presents the paper published in the Journal of Autonomous and Adaptive Communications Systems – IJAACS by Inderscience Enterprises Ltd. 2009. The title of this paper is 'A secure service architecture to support wireless vehicular networks'. This chapter defines the elements of the district service architecture which supports the delivery of temporary session service attributes.

6.1 Abstract

6.1.1 Résumé en français

Les éléments clés pour les VANETS ont été étudiés dans ce travail pour les communications véhiculaires. Ces éléments peuvent servir de base pour identifier les composants principaux dans un cadre de service approprié. Nous proposons une architecture de service qui comprend la présence d'autorités publiques et privées pour fournir une communication sécurisée. L'objectif de cette architecture est la livraison de services d'informations sécurisées offerts sur demande au bord de la route. Dans cette étude, nous décrivons deux types de scénarios de service: un saut et multi-saut. Les travaux futurs de recherche devront être orientes sur l'approvisionnement de services qui ont un potentiel prometteur pour le déploiement futur d'applications commerciales dans les VANETS.

6.1.2 Abstract

Key elements and different existing approaches intended for VANETS were studied in this paper dealing with security, identity privacy and accounting issues. These issues can serve as

the basis for identifying the main components of an appropriate service provisioning framework. It is proposed a secure service provisioning architecture which comprises the presence of public and private certificate authorities collocated with banking modules. The purpose of this architecture is to facilitate the delivery of information services offered at the roadside infrastructure. In this study, it is described two types of delivery scenarios: single-hop and multi-hop. These scenarios provide a more detailed view on how secure service provisioning can be implemented and what type of challenges might be tackled. Future research work needs to be focused on service provisioning which has a promising potential for the future deployment of commercial applications in VANETS.

6.1.3 Index terms

Vehicular networks, AAA models, service provisioning, security, privacy, billing.

6.2 Introduction

Vehicular ad hoc networks (VANETS) are networks that are enabled by short to medium-range communication systems for vehicle-to-vehicle (V2V) or vehicle-roadside (V2I) communication. The potential benefits associated to enabling road-safety applications through VANETS are well known. This type of applications includes real-time collision avoidance warnings, as well as the exchange of driving parameters among vehicles for a safer driving. Besides these useful and sometimes vital functionalities, another trend of applications which involves commercial non-safety related services is also envisioned by sharing the vehicle communication channel with decentralized mobile applications from different service providers. The array of these commercial services can be broad, ranging from internet access, vehicle infotainment, navigation assistance to transportation logistics management. The success of service provisioning models for VANETS from a commercial perspective depends on the implementation of robust architectures that are able to maintain their overall performance when facing different real vehicular situations. In particular, new challenges arise concerning security mechanisms, privacy of user information, and billing for services in a highly mobile and sometimes multi service environment. A key point for maintaining robust service provisioning resides in the capacity to manage a series of security mechanisms which comprise authentication and authorization of subscribers who possess dynamic behaviours. These mechanisms must provide to the communicating parties a secure way to exchange information. Additionally, service providers can regulate the provisioning of their services by implementing specific user profiles, as well as defining service delivery policies supported by their business models. Moreover, in VANETS environments, billing processes can be extended for service message forwarding among vehicles. This can be done by deploying incentive and collaborative mechanisms to foster service delivery independently of the physical location of the destination.

In common information services architectures, the deployment of Authentication, Authorization and Accounting models constitute a fundamental part for the deployment of services mainly used by network operators and e-commerce applications [Housley and Aboba, 2007; Atwood, 2007]. In the VANET context, the distribution of security features must be built around a key management system for authentication purposes. For accessing the network, user authorization might include two levels: first, authorization to access a radio channel at the roadside unit (RSU); second, authorization to access a specific service application at the service provider. Once a user has been fully authenticated, the provider grants him with the right to access the service. This permission can be issued by using service credentials depending on the provider's specific policies. Additionally, an accounting server infrastructure needs also to be available for charging purposes and metering for service consumption. In the following some specific issues that need to be addressed: primarily security, privacy, and billing mechanisms in order to make VANETS service deployment secure for users and viable for service providers (SP).

This work describes a secure service provisioning architecture which support spontaneous on-demand services based on the presence of diverse certificate authorities as well as banking entities which will facilitate the delivery of content data.

6.3 Secure service provisioning for vehicular networks

As mentioned before, access models main tasks are to grant network and service access to users if they meet established access control regulations and to keep the corresponding users' records consistently. These responsibilities are essential part in the development of business models and sustainability of information services. As on-demand services will be mostly open to all public on the road, contents of exchanges between users and service providers must be kept reliable; especially, when user identities are exchanged or financial transactions are performed.

As can be seen in Figure 6.1, it is introduced the notion of Service District domain. A service district is a logical zone that is usually mapped to a map zone where a set of services from different SP are offered. Different elements contained within the administration of the district service entity are logically interconnected between them. The depicted access interfaces are the entrance points for the access routers to the service core. Access routers have two main functions. On the one hand, they connect roadside units which handle communication within the wireless medium. On the other hand, they connect a set of registered information service providers residing at the fixed network. These are just intermediate routers from the RSU to the fixed network. For simplicity purposes access routers can be considered as a part of the fixed network of the service district domain.

In general, authentication is performed in the security module which can comprise the presence of multiple certificate authorities or their corresponding proxy modules. In the proposed architecture, the authentication of communicating participants is guaranteed by providing security features during the initial communication setup between a users and a SP.

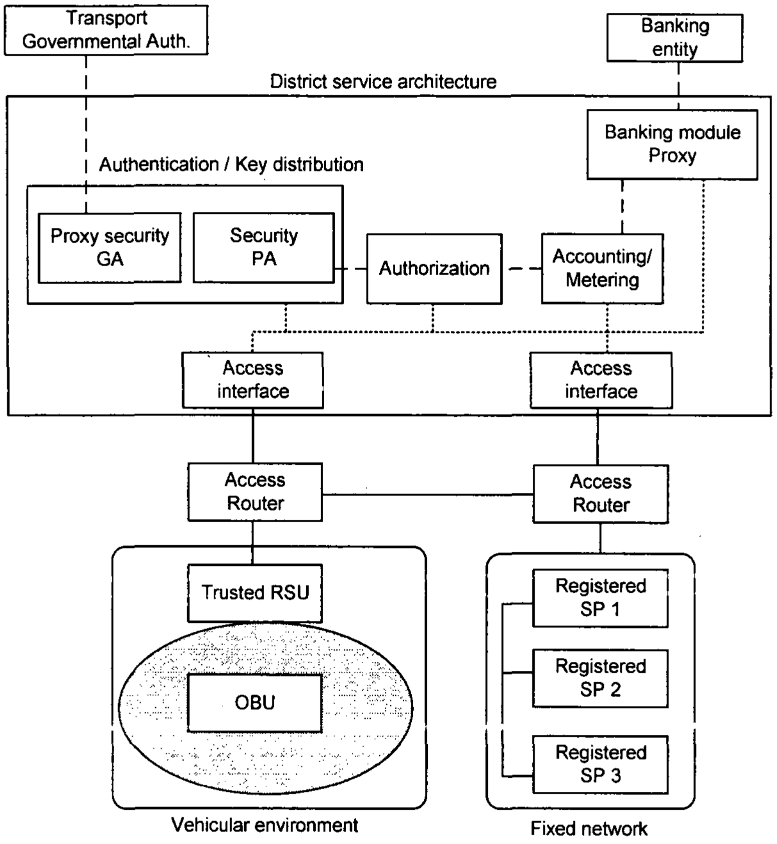

Figure 6.1 - Secure service architecture model

One way to secure communication in highly mobile environments with two communicating vehicles is described as follows:

1. Vehicle *A* publishes its corresponding public key certificate (preloaded by a governmental authority) to vehicle *B*.
2. Vehicle *B* generates a hash function to share a secret key K_{AB} with vehicle *A*.
3. Vehicle *B* encrypt secret key with vehicle *A*'s public key.
4. Vehicle *A* decrypts with its own private key the received shared secret key K_{AB}.
5. Both vehicle *A* and *B* have the shared secret key to encrypt and decrypt messages.

In the proposed architecture some assumptions have been considered. First, the security module must be capable to support and classify different types of requests depending on their priority and/or delay susceptibility. For some situations, the security module must rely just on the validation of the disclosed certificates by the requester without generating any kind of temporary cryptographic keying material. Second, on-demand services do require temporary cryptographic keying material in order to support content delivery. To verify the non-revocation state (certainty) of the disclosed requesters' certificates [Housley *et al.*, 2002], the following steps have to be considered:

A. Verification of the user transit related certificate based on public transit Certificate Revocation lists (TCRL) which contains the serial numbers of the revoked transport official certificates and pseudonyms. For validation of user's certicates, CRLs are required to detect any compromise certificate.

B. Verification of the user temporary related certificates based on local private certificate revocation list (PCRL), it also contains the serial numbers of the revoked temporary certificates and pseudonyms (on-demand services).

C. If verification succeeds; security attributes for the requested session are generated for on-demand services.

Now, to secure the content of the new temporary cryptographic material (session key and pseudonyms) generated by the *PA*, the main tasks performed by the *PA* are enlisted as follows.

1. Issuing of $K_{session}$ session key, *PA*'s certificate and signature, i.e. $Cert_{PA}$ $\{PK_{PA}, SIG_{Priv/PA}$ $(PK_{PA})\}$, where PK_{PA} is the *PA*'s public key and $Priv_{PA}$ is *PA*'s private key

2. Pseudonyms are generated by the *PA* as PID_1 for the user and PID_2 for the corresponding service provider.

3. Encyption by using the shared secret key ($K_{PA/user}$) to protect the dispatched security attributes, involving the new pseudonym, timestamp and session key, i.e. $Enc_{KPA/user}[PID, timestamp, K_{session}]$. The *PA* is in charge of generating the active shared key for both the user and service provider.

4. The *PA* builds associations between the user's captured pseudonym, the new pseudonym (*PID_1*), timestamps and common session key.
5. The *PA* builds associations between the providers's captured pseudonym, the new pseudonym (*PID_2*), timestamps and common session key.

In this process, it is considered that temporary session keys hold short validity periods for the purpose of short frequent update periods; hence, increasing the security level during the session. If the priority of the message does not deal with safety purposes but with consumption of information services; then, it must be a requirement to count with the presence of banking entities, as well as, accounting elements which need to be in place to ensure revenues for service providers. In general, any kind of information exchange related to banking transaction must be collected and analyzed. As can be seen in service architecture, banking entities shall be responsible for extending on-demand credit units in order to grant the use of information services, as well as for issuing banking and service consumption policies. The accounting module contains specific policies which define the way resources are utilized for a given user and also for the type of service requested.

It is assumed that there must be a pre-established relationship between the banking entity and the user for validation purposes which can be based either on user id or some specific banking credentials. Validation of the requester by the banking entity is performed after the authentication of communicating parties has been completed; that is, when session keys are available for the provider and the user. Once the validation of the user is performed by the banking proxy module and if successful, the banking entity is able to dispatch corresponding credit units which can specify the amount of content data to be retrieved or maximum duration of the service session.

A challenge to tackle arises within the vehicular environments given the ad-hoc behaviour of neighboring nodes, and collaboration of nodes may be necessary for the delivery of information up to the final destination. As a result, a reliable incentive scheme distributed through the forwarding path among the participating nodes must be deployed. Additionally, reputation systems can be implemented along the forwarding chain to monitor the correct delivery of packets. The SET (Secure Electronic Transaction) scheme is not considered in this proposal due to the incentive scheme is intended to be delivered in multi-hop environments, which is not the case for the SET.

6.4 Single-hop session attributes

This might be the typical case of information service deliveries where the vehicle has relatively slow mobility or is within proximity before a nearby roadside unit (RSU); the service session can then be established within the radio transmission range. One of the most likely technologies to be considered for a wide deployment in urban and rural areas is Direct Short Range Communications (DSRC). A feature of this technology is that it supports seven service and two control channels where the services offered are frequently broadcasted by an operating RSU. Roadside units are assigned with public key issued by the administrative authority. Public certificates are validated by its digital signature. This set of services is contained in a list called Provider Service Table (PST).

For the analysis of this scenario, it is considered an on-demand service request where services are openly offered to transitory vehicles (see Figure 6.2). First, it is assumed that a potential on-board unit (OBU) obtains the PST information which was broadcasted by RSU within the radio transmission area. The OBU sends an initial message to the RSU notifying its presence. Then, the RSU can reply to the message by requesting the OBU's security attributes. Initially, the OBU transmits a signed service request message to RSU A containing its preloaded pseudonym, public key certificate, current time and the service identifier retrieved from the PST list (step 1). Note, that sensitive information such as pseudonyms and key certificates is encrypted by using the pre-shared key between the OBU and the *PA*. Pseudonyms are associated with its corresponding public key certificate. At the RSU, the signed message request is verified by using OBU's public key and then passed to the access router (step 2). Notice that for the sake of simplicity, it is considered that the RSU and SP share the same access router. At the access router (AR), the OBU's service request is parsed and the service identifier is matched with a specific SP name and identifier, as well as the PA's address. A request message containing the current OBU's pseudonym and key certificate is forwarded from the AR to the *PA* (step 3). Once the *PA* receives the request message, the preloaded pseudonym needs to be verified by the *GA* by sending a validation request message. Forged pseudonyms can be detected since the *GA* is responsible of issuing official security attributes for all vehicles. As soon as the validation is retrieved, the *PA* is able to generate the pseudonyms and session keys for the OBU and the SP, respectively (step 4). Before distributing this security attributes to the OBU and SP, a validation by the banking, accounting and the authorization modules might be performed (step 5).

Depending on the type of banking policies applied, the OBU might be requested to disclose its banking credential which serves as an identifier for its verification and possible eligibility to get credit units issued. This process assumes a secure path by encrypting baking credentials through a pre-shared key between the banking proxy and the OBU. Banking credential and pre-shared key must match otherwise the information sent by the user to the banking proxy cannot be retrieved. Once the validation at the banking module takes places and succeeds, a set of banking credit units is issued for the OBU of the service. For accounting purposes, an association with the current pseudonym, service utilization and banking attributes must be created. At this point (step 6), all the information pertaining to the OBU and the SP is collected by the *PA* and encrypted with the pre-shared keys $K_{PA\text{-}obu}$ and $K_{PA\text{-}sp}$, as well as, appended with the corresponding PA's public key certificate, respectively.

1. $Cert_{PA\text{-}obu}\{PK_{PA}, Timestamp, Enc_{Kpa\text{-}obu}\{PID_{obu}, credit, K_{session}\}, SIG_{PA}[PK_{PA}]\}$
2. $Cert_{PA\text{-}sp}\{PK_{PA}, Timestamp, Enc_{Kpa\text{-}sp}\{PID_{sp}, credit, K_{session}\}, SIG_{PA}[PK_{PA}]\}$

The composed secure message is forwarded back to the corresponding recipients via the AR (step 7-8). At this point, a secure service delivery process can take place by employing the secret session key between the OBU and the SP (step 9).

Notice that during this process, there are no distinctions between a user and OBU; even though, it is likely to have a one-to-many relation where one OBU can be shared by multiple users. In this case, it is considered a one-to-one relation where one OBU corresponds only to one user to simplify the scenario illustration.To minimize the risk of eavesdropping activities that correlate the temporary pseudonyms with actual user identities by malicious parties, it is possible to consider changes of pseudonyms on a time-based expiration scheme during the service session. That means that the user will need to request a new set of secure attributes to the *PA* when the current ones have already expired. In general on this provisioning model, authentication, integrity and non repudiation requirements are guaranteed at each connection point.

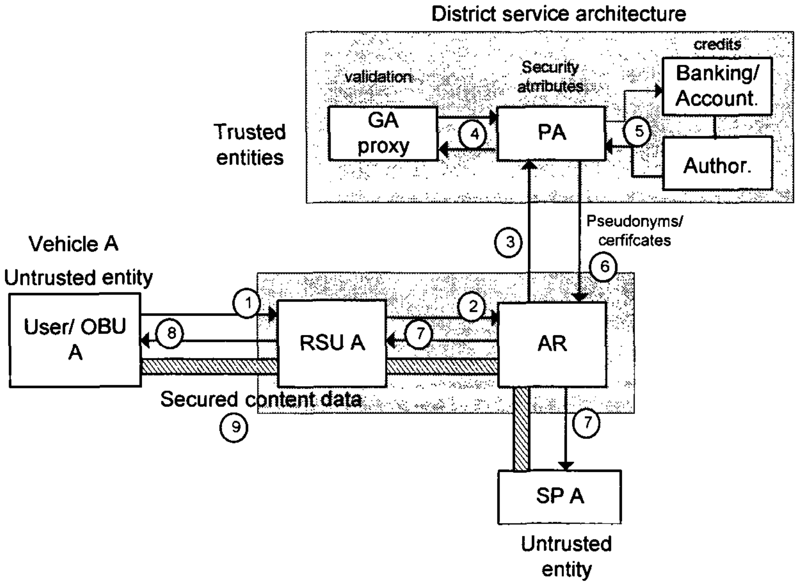

Figure 6.2 - Schematic service authentication and content delivery

6.4.1 Analysis of a single-hop scenario

In this section, it is addressed the total time needed to perform a typical request-response in a single hop scenario for a vehicle requesting access to a service. This process involves the steps 1-9 described earlier. Time is critical for vehicular connectivity because of the high mobility of the connecting node (vehicle). In order to represent the exchange of messages in the proposed architecture, it is used the Application Characterization Environment (ACE®) whiteboard from the OPNET® modeler P14.5 wireless suite [Opnet, 2008]. The ACE whiteboard is a robust tool suitable to evaluate the behaviour of different tier processes within a simulation environment. For this analysis, it is considered cumulative processing time at each stage of the communication model which has to deal with the execution of cryptographic operations. These processing time values are based on the benchmark speeds given in [Crypto++, 2007] for different cryptographic schemes. These time values are used as references in order to estimate the total response time during a simulated on-demand requesting process. The corresponding time values are shown in Table 6.1.

Table 6.1 – Crypto++ benchmark time values

Operation schemes	**Processing Time (ms) per operation**
RSA 1024 signature	1.42
RSA 1024 verification	0.07
RSA 1024 encryption	0.07
RSA 1024 decryption	1.52
DH 1024 key generation	0.44
HMAC(SHA-1)	6.279/byte

From Table 6.1, digital signatures are based on the RSA cryptographic algorithm with a fixed length of 128 bytes. The corresponding signature verification processes are performed by each tier stage, as well as, related encryption/decryption operations when transmission sensitive information is required. Moreover, HMAC operations are necessary when generating pseudonyms (32 bits) at the OBU and at the authentication tiers, respectively. For key generation, the Diffie-Hellman (DH) algorithm can be employed at the authentication tier. Recall that security associations are performed at the security module.

Regarding connectivity parameters, the bandwidth for the fixed network is set to 1 Gbps while the bandwidth for the OBU is set to 54 Mbps given the maximum data rate allowed in DSRC. The maximum packet length was set to 1024 bytes. Furthermore, it is assumed 20 ms latency at each tier process for additional processing operations besides the processing time values inherent to cryptographic operations. Notice that the time for an OBU to discover a RSU in the proximity is not considered, neither is the time for the RSU to broadcast discovery parameters in its surroundings. The objective of the analysis is to quantify the total response time needed to request on-demand services.

As can be seen in Figure 6.3, the total response time is represented on a time scale on the top of the chart which helps to visualize the performance of the entire tier process. From this chart, the elapsed time for a user to retrieve the appropriate access and security attributes from the fixed network is around 0.7 s; where the highest consumption of processing time resides at the authentication tier given the generation of keys, pseudonyms and verification tasks. The obtained value (0.7 s) is acceptable for the purpose of the scenario even if the vehicle is travelling at highway level speeds. Therefore, the value is acceptable, if:

a) After the request is responded to, the vehicle even at high speed is still within the reach of the same access point.

b) From the user point of view the perception of the connection to the service is instantaneous.

Let us consider for example a vehicle moving at speeds reaching 140 km/h, which is the maximum speed supported by DSRC, and also a service coverage range of 500 m realistically offered by the current RSUs of the same technology, given constraints such fading due to topology. If it assumed the existence of adjacent RSUs, overlap zones can be of a recommended 15% (75 m) at both sides of the service zones. In 0.7s, and with a maximum speed of 140 km/h, a vehicle would have travelled an additional 28 m. Of course, to allow seamless handover transitions, a mechanism capable of detecting current access parameters and updating the access associations from the previous RSU to the new RSU shall be present.

Additional analysis has been performed in this study by building a network topology in the Opnet Wireless Project Editor. The objective is to deem the performance of the system when increasing the number of requests which are handled at the service architecture. To implement this topology, an ACE file was used which contains the sequence of messages and their corresponding tier processing times, as a customized task configuration in the Project Editor. Figure 6.4 shows the network topology as implemented in the Project Editor. The tier elements are represented as LAN workstation devices while the OBU is represented by a WLAN mobile device. The starting simulation time was set at 100 s and the application profile is configured to handle inter-repetition executions for the duration of the simulation time. Additionally, the application profile was set to support concurrent request messages; therefore, this can reflect the impact on the application processing when increasing the number of mobile nodes. Moreover, the total simulation time is set to 20 s and mobile nodes are configured with an urban speed of 60 km/h. As can be seen in Figure 6.5, the average response time for a single node, 15 and 30 nodes become around .71 s, .73 s and .75 s, respectively. From these results, there is a slightly difference on the overall average response time for 30 nodes; therefore, the obtained values remains appropriate for those traversing nodes requesting services along the service coverage area.

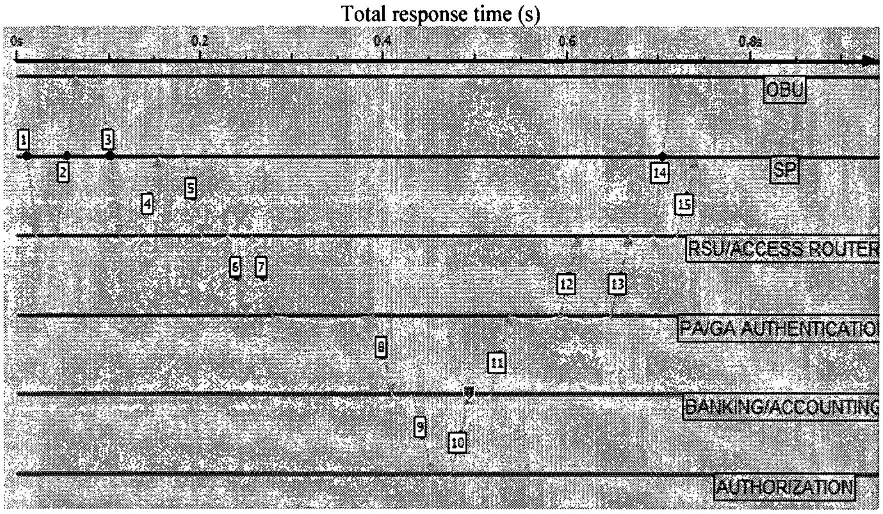

Figure 6.3 - ACE whiteboard message tier process

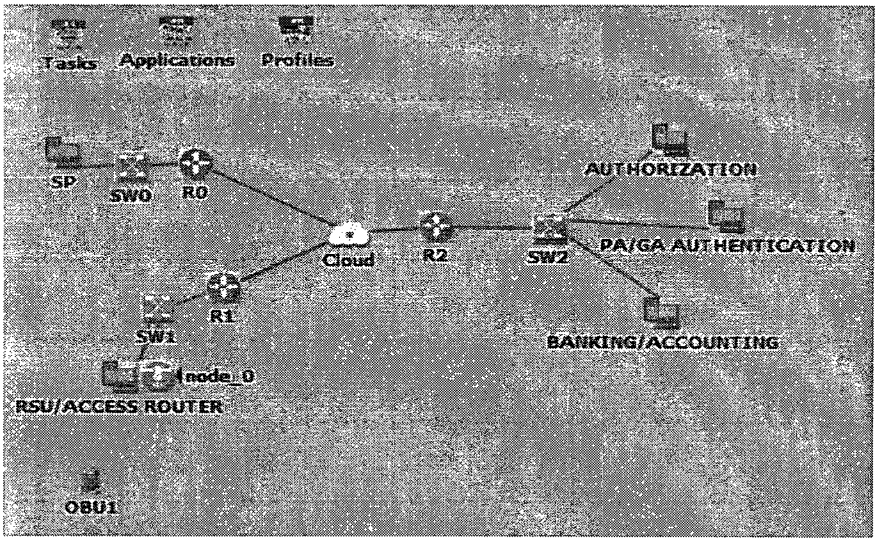

Figure 6.4 - Network topology

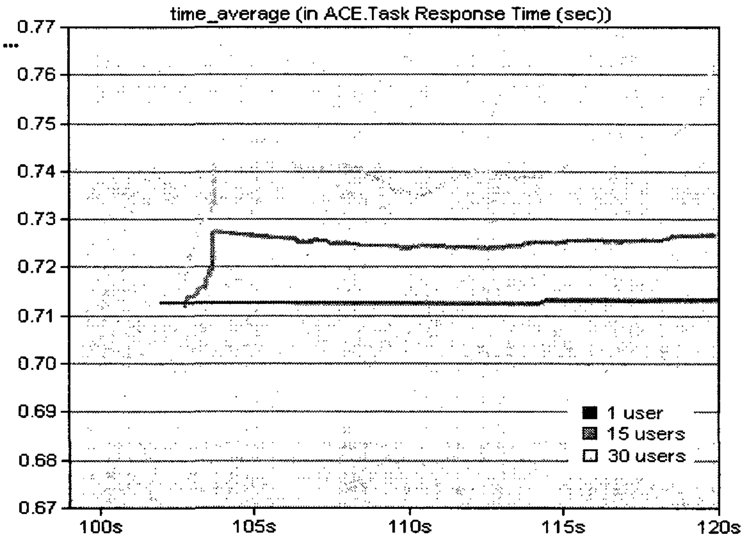

Figure 6.5 - Single-hop average time response

6.5 Promoting multi-hop collaboration

For the analysis of this scenario, it is necessary to focus on the distribution of incentive units along the multi-hop path when the messages have to be propagated beyond the limited radio transmission area in order to get to destination.

Basically, at the secure service architecture the validation and generation of security attributes for the corresponding user and the SP follows the same procedure as in the single-hop scenario. The difference relies in the ad hoc environment where sensitive information is encrypted at the authentication phase by using the secret key between the user and the *PA*. For the payload delivery phase, the information is encrypted by using the temporary session key between the user and the SP. In either case, there is no chance for intermediate nodes to extract the contents of the transmitted message since they do not have the corresponding keys to decipher the messages. Then, the main tasks to be performed by intermediate nodes are to validate the preceding sender's signature by using the corresponding neighbour's public key certificate and to forward the packet with the current node's signature.

Based on the forwarding path followed during the initial authentication process, banking entities can provide bonus units along with timestamps for those nodes participating in the forwarding path. These incentive units promote active participation of neighbouring nodes and can serve as cumulative benefits for later rewards. Some kind of incentive is necessary as local resources are utilized at every single forwarding node in order to deliver the payload messages up to the final user.

Along the path, it is considered that a chain of certificates must be built through public key certificates for every single intermediate node (see Figure 6.6). At the banking entity, there is an association between a bonus unit and its corresponding public key certificate which also serves to encrypt the dispatched bonus units and respective timestamps. Consequently, at every forwarding node, the current node will be able to decrypt the bonus unit by using the corresponding private key. The following list summarizes the above procedure.

1. Intermediate node$_i$ sends public key certificate $Cert_{OBUi}$.
2. At the banking module, bonus unit and Timestamp (Ts) are encrypted with node$_i$ public key certificate, $Enc_{kcertOBUi}\{bonus_i, Ts\}$
3. At intermediate node$_i$, message is decrypted with node$_i$'s private key, $Dec_{kprvOBUi}\{bonus_i, Ts\}$.

Additionally, each node must have a specific buffer to store all received bonus units. However, there is an open issue to solve in the way that what if the *n*-node accepts the bonus unit but it fails to deliver payload packets. For now, it is assumed that the delivery of packets through the intermediate *n*-node is guaranteed. Clearly, this assumption possesses the risk of getting bonus units without participating in the packet delivery. For the ad hoc environment, some possible solutions can come with the deployment of reputation systems such as watchdog [Fonseca and Festag, 2006] in charge of monitoring the forwarding behaviour of every single node in the delivery path. If an intermediate node fails trustworthiness, this node is discarded from the forwarding path. Appended certificates are required to assure collaboration and generation of incentives. A description of different ad hoc routing protocols can be found in Appendix A.

In summary, the exchange of service messages is secured at every forwarding point. This procedure can guarantee that the message is legitimated by the participating intermediate nodes along the path from the user to the SP. Furthermore, this scheme promotes collaboration between nodes through the use of incentives issued at the fixed infrastructure. Appended certificates are required to assure collaboration and generation of incentives. Recall that the access protocol requires this forwarding list of intermediate nodes, but the payload traffic is not affected by the overhead caused by the appended certificates.

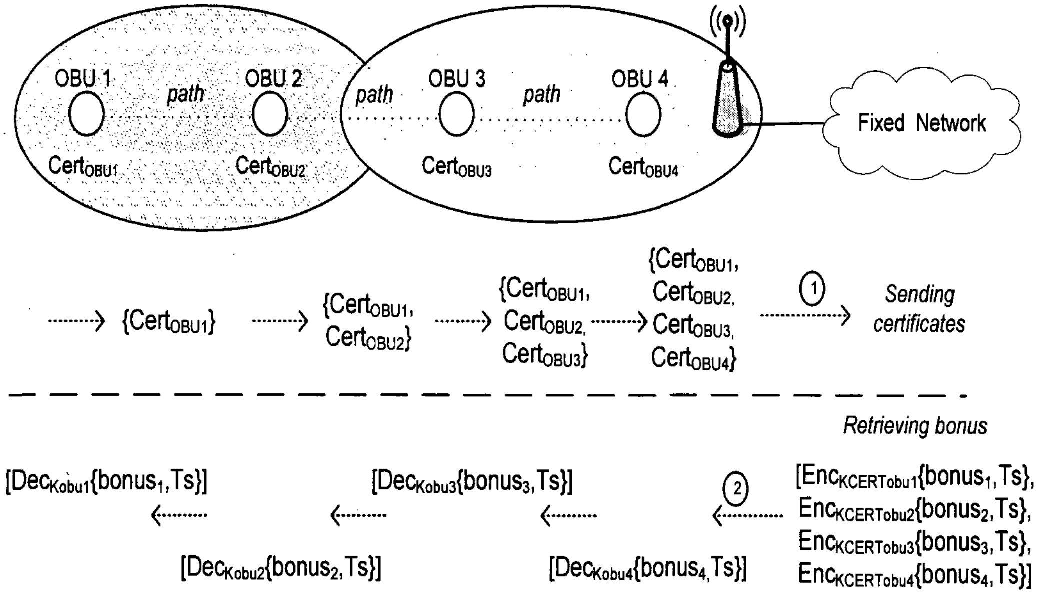
OBU 1
path
OBU 2
path
OBU 3
path
OBU 4
Cert_{OBU1}
Cert_{OBU2}
Cert_{OBU3}
Cert_{OBU4}
Fixed Network
$\{\mathrm{Cert}_{OBU1}\}$
$\{\mathrm{Cert}_{OBU1}, \mathrm{Cert}_{OBU2}\}$
$\{\mathrm{Cert}_{OBU1}, \mathrm{Cert}_{OBU2}, \mathrm{Cert}_{OBU3}\}$
$\{\mathrm{Cert}_{OBU1}, \mathrm{Cert}_{OBU2}, \mathrm{Cert}_{OBU3}, \mathrm{Cert}_{OBU4}\}$
1
Sending certificates
Retrieving bonus
2
$[\mathrm{Enc}_{KCERTobu1}\{bonus_1, Ts\}, \mathrm{Enc}_{KCERTobu2}\{bonus_2, Ts\}, \mathrm{Enc}_{KCERTobu3}\{bonus_3, Ts\}, \mathrm{Enc}_{KCERTobu4}\{bonus_4, Ts\}]$
$[\mathrm{Dec}_{Kobu4}\{bonus_4, Ts\}]$
$[\mathrm{Dec}_{Kobu3}\{bonus_3, Ts\}]$
$[\mathrm{Dec}_{Kobu2}\{bonus_2, Ts\}]$
$[\mathrm{Dec}_{Kobu1}\{bonus_1, Ts\}]$

Figure 6.6 - Distribution of incentives in multi-hop scenario

6.5.1 Analysis of a multi-hop scenario

For this scenario, the benchmark values are taken for cryptographic operations given in Table 5.1. It is also considered an average propagation delay between two nodes of 20 ms, as experimented by [Eichler *et al.*, 2004], when using AODV protocol for vehicular ad hoc routing. The processing time regarding each intermediate node in a multihop path corresponds to the time required for signature generation, as well as verification of signatures from neighbours. In the response message from the fixed network for the mobile source, an additional decryption process must be considered at each intermediate node in order to decrypt the information (bonus) issued by the banking entity. Recall that incentives are intended to promote forwarding among participating nodes.

As can be seen in the time scale on top of the chart in Figure 6.7, the total response time required for the user to retrieve the appropriate access and security attributes from the fixed network when there are four hops is around 1.3 s, where the highest consumption of processing time still resides at the authentication tier.

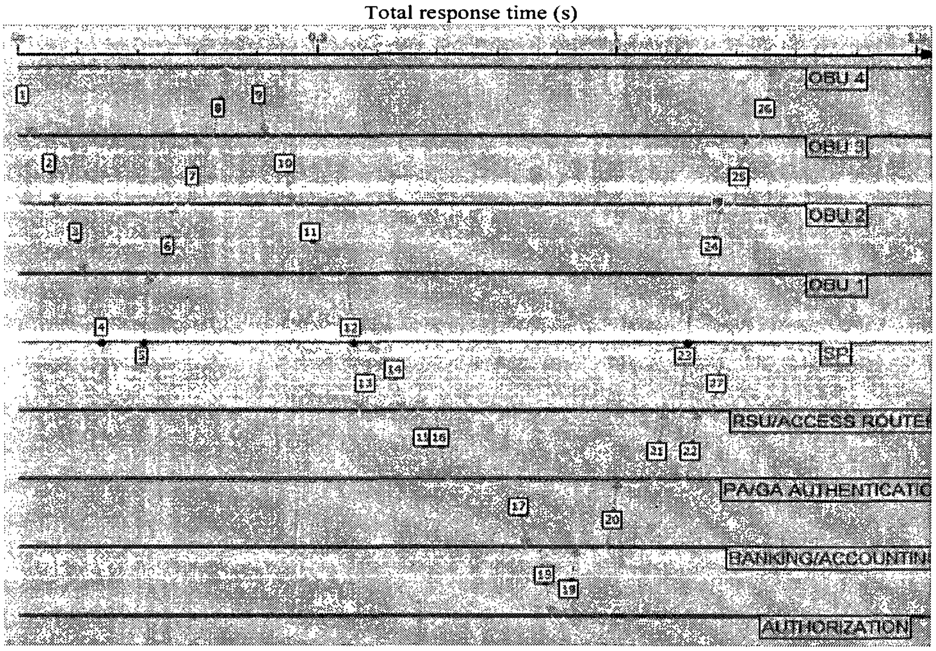

Figure 6.7 - ACE whiteboard message multi-hop tier process

Following the same reasoning as in the high speed single-hop scenario, it might be considered a group of 4 vehicles traveling at an average speed of 140 km/h within a service range of up to 500 m; then, in 1.3 s, and with a maximum speed of 140 km/h, a vehicle requesting service would have travelled an additional 50 m, and the same for the last hop. With 4 hops in the propagation path, the total time response should still be acceptable.

Additional analysis has been performed by implementing the ACE multi-hop tier process in an ad hoc topology. The mobile nodes are located with a separation distance of 500 m between each other and are configured to support the AODV routing protocol. The mobile nodes are also configured with an urban speed of 60 km/h. In the simulation setup, the RSU is represented by a MANET base station device which is a gateway which can support the AODV routing protocol. The starting simulation time was set at 100 s and duration time of 10 s. The application profile is configured to handle inter-repetition executions for the duration of the simulation time. These are the results for a single request message in multiple-hops, is not for streaming payload traffic in a multihop environment. As can be seen in Figure 6.8, the average response time for three, five and 10 intermediate nodes become 1, 1.5 and 2.2 s, respectively. As expected when introducing additional intermediate nodes, the average response time increases.

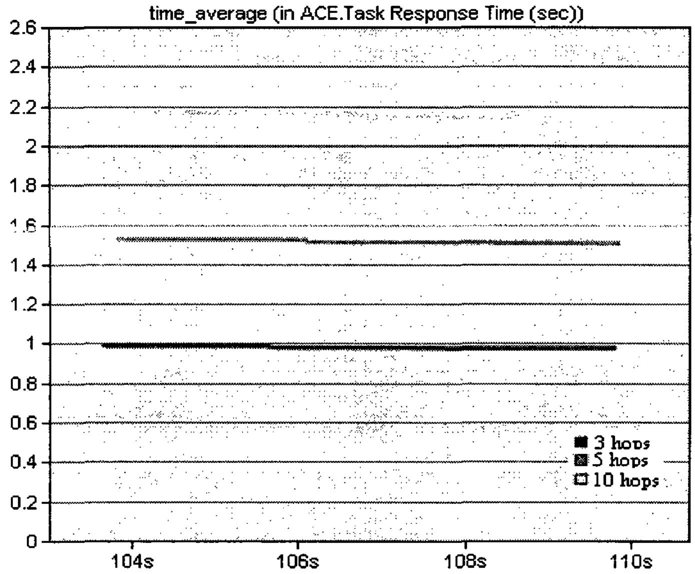

Figure 6.8 - Multi-hop average response time

6.5.2 Discussion

Major challenges dealing with transitory and dynamic behaviour of users must be tackled in order to offer consistent services on the road on an on-demand basis. The main premise is that the user might request services anytime, anywhere and without being attached to a home network provider. In order to support commercial applications, charging operations must be executed to validate the affordability of the potential user, as well as, to guarantee a secure service delivery. The advantage of implementing robust security schemes becomes evident, especially, when sensitive information has to be delivered in a vehicular environment, and also to make service provisioning viable for service providers. Security becomes also priority when information needs to be forwarded through unknown and at the same time not trusted vehicles. With this proposed architecture, data is protected at all times and keeps the key features of any protected communication; that is, integrity, authentication and non-repudiation. Moreover, the use of temporary pseudonyms increases protection against possible privacy attacks. An additional issue that might arise is the possible control and regulation of services and their policies by official authorities. This can represent an overwhelming structure in the way services are offered and granted, especially, in the case when user privacy might be affected since official authorities are the ones who validate public certificates.

To the best of our knowledge, no other works have estimated such response delay for accessing services in complete tier process architecture for vehicular networks as it is presented in this study. The simulation studies performed for the architecture show that the delay overhead due to service access is acceptable for both single-hop and multi-hop scenarios even when vehicles travel at high speeds and the number of requesting vehicles increases. Evidently, the longer a forwarding path, the longer the delay for security processes to take place; which may lead to disconnecting from an access point before a response is delivered back to the requesting vehicle. Additionally, an unstable forwarding topology among vehicles would have a significant impact in the forwarding path which facilitates the request-response process through intermediate nodes. Disconnections among forwarding vehicle may hinder long term sessions between a requester and a provider.

6.6 Conclusions

In this chapter relevant characteristics and models for service environments in the vehicular context have been presented. The major concern is to provide a robust and secure transfer of information between a vehicles and a provider. Key elements regarding the implementation of service provisioning in VANETS and different existing approaches were studied concerning security, identity privacy, accounting and billing issues. It is worth noting that most of the existing security approaches propose PKI infrastructure given the possible compulsory requirements imposed by VANETS. These previous elements served as the basis for identifying the main components of an appropriate service provisioning framework. It is proposed a secure service provisioning architecture which comprises the presence of public and private certificate authorities collocated with accounting and banking entities. The purpose of this architecture is to facilitate the delivery of information services offered at the roadside infrastructure. The main goal of the security module is to verify the certainty of the holder's key certificates and pseudonyms by using certificate revocation lists. Additionally, the security module must generate the corresponding secure attributes for the user and the service provider as well. These attributes comprise the generation of a shared session key where payload data can be protected and also the distribution of the corresponding temporary pseudonyms.

One major issue when implementing billing models for VANETS is the integration of robust mechanisms that can be implemented at the infrastructure level and also at the vehicular environment. This proposal provides incentives in the form of bonus units for those participating vehicles which contribute in the delivery of information through the forwarding path. Incentives could represent potential benefits for future banking transactions. The simulation studies performed for the architecture show that the delay overhead due to security mechanism is acceptable for both single hop and a typical multihop scenario even when vehicles travel at high speeds. Long term connectivity becomes an issue in multihop scenarios. Solutions may need to integrate robust architectures to support the interaction of multiple RSUs which can handle seamless handover operations, efficient security mechanisms, and also efficient ad hoc delivery.

The next chapter details the analytical model of an extended service district architecture and analize the corresponding cost in terms of delay and performance when increasing the numbers of users. [Coronado and Cherkaoui, 2009].

CHAPTER 7

JOURNAL OF SECURITY AND COMMUNICATION NETWORKS, WILEY 2009

This chapter presents the paper published in the Journal Security and Communication Networks by Wiley-Blackwell. The title of this paper is 'Performance Analysis of Secure On-demand Services for Wireless Vehicular Networks'. This chapter covers the analytical model and performance for on-demand services for different vehicular communication scenarios.

7.1 Abstract

7.1.1 Résumé en français

Ce travail adresse les paramètres nécessaires pour offrir des services sécurisés sur-demande aux usagers véhiculaires au bord de la route. Trois types de protocoles de demande de service sont introduits dans notre travail pour le cas d'un saut (SHI-RQ), connectivité étendue (CE RQ) et multi-saut (MHI-RQ). Le modèle analytique et l'étude de coût pour les protocoles sont présentés. Notre analyse couvre le coût total de la latence pour chaque protocole d'accès. L'analyse rend compte des caractéristiques de mobilité et de densité des véhicules voyageant à travers les domaines de service. Les résultats analytiques montrent des coûts acceptables pour un nombre réaliste de véhicules voyageant aux vitesses permises sur la route.

7.1.2 Abstract

Wireless vehicular communications pose significant challenges for the deployment of next generation roadside services. Some important issues that must be tackled are security, billing and reliability while guarantying a scalable service delivery. This paper addresses the assignation of secure service session parameters upon the reception of on-demand service requests by an incumbent services district domain and studies and analyses the performance of the underlying mechanisms. Three types of service request protocols are introduced in this work defined as single-hop (SHI-RQ), extended connectivity (EC-RQ) and multi-hop (MHI-RQ) service requests. A detailed analytical model and cost study for the access protocols are presented. The analysis covers the estimation of total cost in terms of latency for each access protocol with different mobility characteristics and vehicle densities within the service coverage area and across different serving district domains. The analytical results are consistent with the experimental one and show that the signaling cost in terms latency remains acceptable for a realistic number of serviced vehicles even at high speeds.

7.1.3 Index terms

Vehicular networks on-demand services, service provisioning, security, billing.

7.2 Introduction

Vehicular ad hoc networks (VANETS) are networks that are enabled by short to medium-range communication systems for vehicle-to-vehicle (V2V) or vehicle-roadside (V2I) communications. The main difference between safety and commercial applications relies in that a prospective requester must be subjected to a verification of his affordability to retrieve a service. On this regard, billing mechanisms in vehicular environments must be designed in order to grant the right to use of an intended service. The array of these commercial services can be broad, ranging from internet access, vehicle infotainment, navigation assistance to transportation logistics management. The potential of vehicular communications will rely on the way services are discovered, accessed and they are kept reliable through different wireless technologies. All these factors are likely to determine how business models are offered at the roadside infrastructure and how these solutions can be maintained scalable through different network domains.

In this work it is defined signaling protocols based on service architecture proposed in [Coronado and Cherkaoui, 2008] which is intended to offer secure service provisioning for spontaneous on-demand service requests. The main motivation is based on the premise that vehicles may request services anytime, anywhere and without being attached to any sort of home network. For this work, it is analyzed the performance of the signaling cost of the proposed protocols carried out between the requester and the service district domain.

The rest of this chapter is organized as follows. A description of the elements comprising the service district domain architecture is given followed by the message notation of the proposed signaling protocols. An analytical model with expressions of the corresponding signaling costs, followed by the analysis of the mobility model and numerical results are presented. Finally, this work ends with the conclusions.

7.3 Service district domain architecture

In this section, it is explained the main signaling protocols involve in the request of on-demand services offered on the road and which requests are processed by the serving administrative service architecture. First, it is defined the service district domain as a logical zone that is mapped to a geographical area where a set of services from different roadside providers are broadcasted by the wireless infrastructure. As can be seen from Figure 7.1, elements contained within the administrative control are logically interconnected between them. These elements are in charge of processing and validating incoming requests from potential users. Given the fact that transitory users can possess high mobility and sometimes unpredictable trajectories, the service district domain may not have knowledge in advance of the potential user; therefore, the district domain has to rely in specific mechanisms suitable for this kind of environments. In the depicted architecture, access routers are illustrated as part of the core network but their main function is to provide connectivity to the RSU based on DSRC technology and the registered service providers.

Authentication of the public key certificates disclosed by requesters relies on the validation of the non-revocation state (certainty) of those certificates through certificate revocation lists. For the analysis, it is assumed that disclosed public certificates include their digital signature; therefore, a verification process of digital signature takes place. Even though, this is an open architecture the distribution of session parameters must be secured at all times to the corresponding recipients by encrypting the information with the user's public key in the case of the user and with a secret shared key between the provider and district domain.

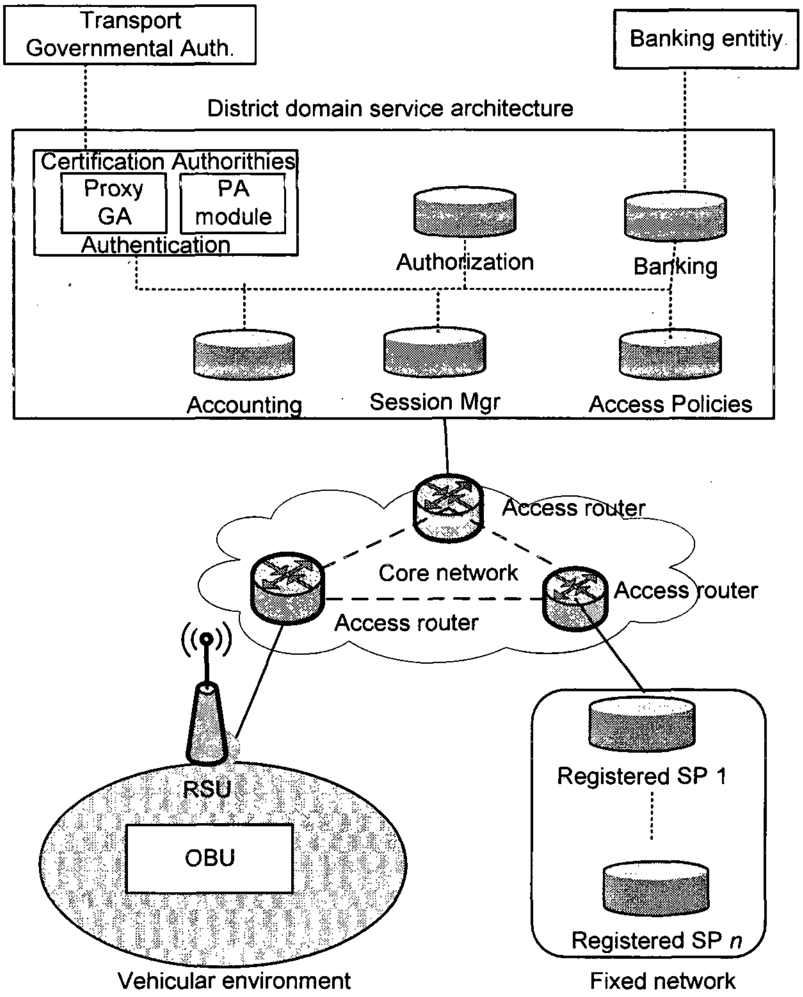

Figure 7.1 - Extended service model

Banking validation resembles a credit-card payment modality where the capacity of the potential user to afford a specific service can be verified by an external banking entity or by a proxy module within the district service architecture. Notice again that validation of the requester by the banking entity is performed after the authentication of potential communicating parties has been successfully completed. Once a successful validation of the user takes place, the banking entity is able to dispatch the corresponding credit units and a transaction identifier that specifies the amount of content data to be retrieved or the maximum time duration for the service session.

Regarding the presence of the session manager, its main function is to establish associations with other external session managers for the purpose of supporting scalability between multiple district domains. Any exchange of information between different district domains will be performed through the interaction of current participating session managers. This module is also responsible of creating a session ID and for collecting all the session parameters before being forwarded to the RSU.

For the establishment of the service request protocols, three main types of request messages must be parsed and executed accordingly by the operating service district domain. The scope of this analysis is based on three main entities at the service district domain which comprise session manager, security and banking modules.

1. Single hop Initiation request protocol *SHI-RQ*. This set of messages is intended to initiate a service request in a single-hop vehicular to infrastructure modality.
2. Extension connectivity request protocol *EC-RQ*. This protocol is intended to provide continuous connectivity when a vehicle changes from one district domain to an adjacent one. Exchange of current session parameters takes place when performing handover operations between different service district domains.
3. Multi-hop Initiation request protocol *MHI-RQ*. This set of messages is intended to initiate a service request in a multi-hop environment.

It is assume that the fixed infrastructure is based on a trusted model which includes the RSU and service district domain architecture. In the following it is expressed the message notation for the aforementioned protocols.

7.4 Single-hop initiation service request protocol [SHI-RQ]

A *SHI-RQ* message identifies a single-hop V2I on-demand service request which is executed by the OBU. First, the OBU sends an initial message to the RSU notifying its presence. And the RSU can reply to the message by requesting the OBU's public key certificates and intended service identifier. It is assumed that the initial exchange of *SHI-RQ* messages is part of the service discovery mechanism. The enlisted message notation described below is illustrated in Figure 7.2 and the definition of acronyms is given in Table 7.1.

1. Once service discovery is completed, the OBU sends an extended request message which includes the service ID which identifies the service the user is willing to acquire; public certificate which includes a digital signature; an encrypted banking credential and sequence number. A digital signature is implicit in the certificate structure; for instance, a certificate (X.509) includes the public key and the digital signature. Recall that there must be a pre-established relation between the prospective user and the banking entity for charging purposes. The costs of services can be distributed such as data cost, operational cost, infrastructure costs meaning profits for the service provider and the owner of the infrastructure (district domain). Digital signatures utilize the user's private key and they are validated by using the user's public key.

$$OBU \rightarrow RSU : Cert_{OBU}, Srv\_id, Enc\{Bnk\_id\}_{K_{bnk-obu}}, Seq_{OBU}$$

2. When the *SHI-RQ* is received at the RSU containing a specific service ID, the RSU sends a request message to the SP for initialization purposes denoted as *SP[SHI-RQ]*. Then, the service provider (SP) replies with its public certificate and sequence number.

$$SP \rightarrow RSU : Cert_{SP}, Seq_{SP}$$

3. The RSU parses and collects the information retrieved from the OBU and SP, respectively; and relays the service request message to the session manager (SM) which resides at the service district domain. Request messages are appended with the requester's certificate (public key and digital signature).

$$RSU \rightarrow SM : Cert_{SP,} Cert_{OBU}, Srv\_id, Enc\{Bnk\_id\}_{K_{bnk-obu}}, Seq_{OBU}, Seq_{SP}$$

4. The SM issues a session identifier which will serve as index for the whole validation process taken at the service district domain for either a successful or a fail attempt during the subsequent validation steps. A relayed message is sent to the SEC module which contains the public key certificates for both the user and SP. Here, digital

signatures are verified and public certificates are checked their revoked status based on the most recent CRL.

$$SM \rightarrow SEC : Cert_{SP,} Cert_{OBU}, SS\_id, Srv\_id, Enc\{Bnk\_id\}_{K_{bnk-obu}}, Seq_{OBU}, Seq_{SP}$$

5. The SEC module relays the users banking parameters for their validation to the banking entity. There must be an association between the user public certificate and the corresponding shared secret key at the banking module; as a result, the banking module can distinguish the appropriate user record and charge the user accordingly to the service requested. If validation of the user's affordability is successful, a limited credit unit (credential) is generated for the specific use of the service; otherwise, the validation process is aborted.

$$SEC \rightarrow BNK : Cert_{OBU}, SS\_id, Srv\_id, Enc\{Bnk\_id\}_{K_{bnk-obu}}, Seq_{OBU}$$

6. After BNK module verifies the affordability of the potential user for that specific session, if successful, the BNK sends back to the SEC module a message including a transaction identifier, timestamp and the encrypted credit unit by using the shared secret key between the user and the BNK.

$$BNK \rightarrow SEC : SS\_id, Srv\_id, Enc\{Crd\_unt\}_{K_{bnk-obu}}, Trn\_id, T, Seq_{OBU}$$

7. Now upon reception of a satisfactory message, the SEC module is capable of generating the serving session key for the user and provider, as well as, the temporary user and provider ID (pseudonyms), respectively. The information intended for the provider is encrypted with a shared secret key between the registered provider and the district domain. The protected session parameters for the user include session ID, encrypted temporary user ID, session key, encrypted credit unit, transaction ID, sequence number and district identifier. All session parameters for the users are encrypted by using its public key. The composed message is sent back to the RSU via the SM which acknowledges the validity of the session.

$$SEC \rightarrow_a SM(1) \rightarrow_b RSU : Enc\{PID_1, SS\_id, Dist\_id, Kss,$$

$$Enc\{Crd\_unt\}_{K_{bnk-obu}}, Trn\_id, T, Seq_{OBU}\}_{K_{OBU}}$$

Now, the protected session parameters for the provider comprise the session ID, temporary SP ID, session key, transaction id, timestamp and sequence number.

$$SEC \rightarrow_a SM(2) \rightarrow_b RSU : Enc\{PID_2, SS\_id, Kss, Trn\_id, T, Seq_{SP}\}_{K_{SP}}$$

8. The relayed composed session parameters intended for the user within the wireless environment is appended with the RSU public certificate.

$$RSU \rightarrow OBU : Enc\{PID_1, SS\_id, Dist\_id, Kss, Enc\{Crd\_unt\}_{K_{bnk-obu}}, \\ Trn\_id, T, Seq_{OBU}\}_{K_{OBU}}, Cert_{RSU}$$

9. The relayed composed session parameters intended for the provider is appended with the RSU public certificate.

$$RSU \rightarrow SP : Enc\{PID_2, SS\_id, Kss, Trn\_id, T, Seq_{SP}\}_{K_{SP}}, Cert_{RSU}$$

Figure 7.2 shows the exchange of messages for the *SHI-RQ* protocol.

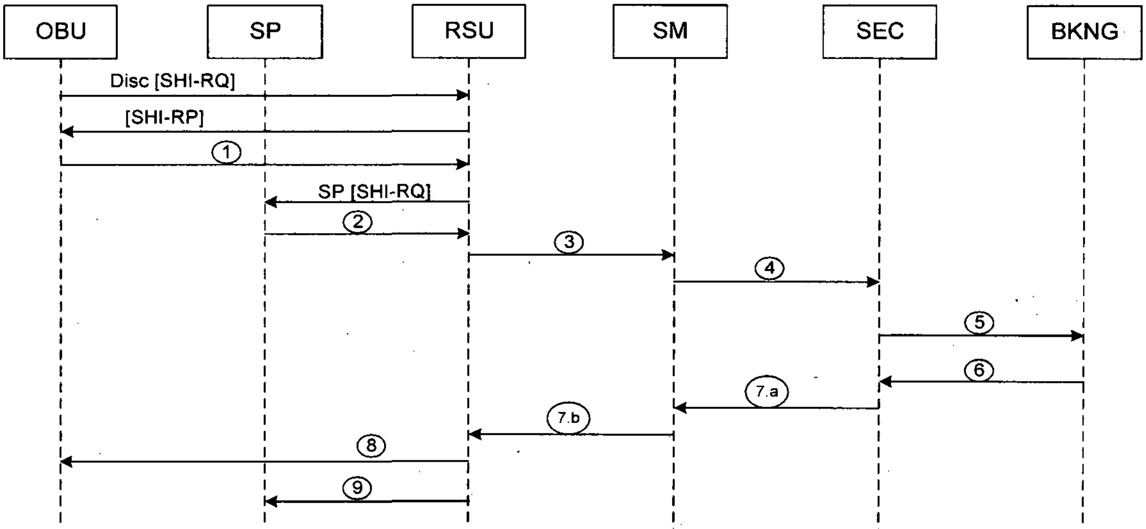

Figure 7.2 - SHI-RQ exchange messages

Table 7.1 – Parameters for on-demand services

Symbol	**Definition**
PID1	User pseudonym
PID2	Provider pseudonym
Kss	Session key
$Cert_{RSU}$	RSU public certificate
$Cert_{OBU}$	User public certificate
Crd_unt	Credit bonus unit
$K_{pa\text{-}sp}$	Shared key authority-provider
K_{user}	User public key
Ss_id	Session ID
Srv_id	Service ID
Trn_id	Transaction identifier
T	Timestamp
$Cert_{SP}$	Service provider certificate
Bnk_id	Banking credential
Seq_{OBU}	User sequence number
Seq_{SP}	SP sequence number
Dist_id	District identifier

7.5 Extension connectivity request protocol [EC-RQ]

1. An *EC-RQ* message refers to the extension of service connectivity request upon a discovery of a new district domain (see Figure 7.3). For this case, the OBU sends an initial *EC-RQ* message to the new discovered RSU$_j$. Then, the recently discovered RSU$_j$ can reply to the message by requesting the OBU its current incumbent district identifier and session ID. Because the *EC-RQ* is a petition of connectivity for an existing session, RSU$_j$ replies with its public key certificate, so the OBU can encrypt its disclosed parameters with the RSU$_j$'s public key. In this case, the OBU sends an encrypted message which includes the current session identifier, temporary user identifier, transaction id, public certificate, district identifier and sequence number.

$$OBU \rightarrow RSU_j : Enc\{Cert_{OBU}, SS\_id, PID_1, Trn\_id, Dist\_id, Seq_{OBU}\}_{K_{RSU_j}}$$

2. Once this encrypted message is received at RSU$_j$, the latter sends an *EC-RQ* request message to SM$_j$ to initiate a connectivity session identifier for the prospective session.

$$RSU_j \rightarrow SM_j : Cert_{OBU}, SS\_id, PID_1, Trn\_id, Dist\_id, Seq_{OBU}$$

3. SM$_j$ contacts SM$_i$ based on the disclosed district identifier in order to validate the session parameters which the user claims to hold. The link is considered to be secured between interconnected session managers.

$$SM_j \rightarrow SM_i : Enc\{SS\_id, PID_1, Trn\_id, Dist\_id, Seq_{OBU}\}_{K_{SM_j-SM_i}}$$

4. SM$_i$ response the request to SM$_j$. If the validation succeeds, a successful message is released (RSP); otherwise, a denial message is issued. Those shared keys are related to the current session manager and the previous one. Communication between session managers must be secured.

$$SM_i \rightarrow SM_j : Enc\{RSP, SS\_id_i, Dist\_id_j, PID_1, Seq_{OBU}\}_{K_{SM_j-SM_i}}$$

5. Once a positive response is received at the new district domain, a new temporary register is created at SM$_j$ to continue offering service continuity. The composed message is encrypted by using the OBU's public key which includes the successful response, new session ID at district j, temporary user and increased sequence number. Recall that a certificate includes the public key and the digital signature.

$$SM_j \rightarrow_a RSU_j \rightarrow_b OBU : Enc\{RSP, SS\_id_j, Distr\_id_j, PID_1, Seq_{OBU}\}_{K_{OBU}}$$

Figure 7.3 shows the exchange of messages for the *EC-RQ* protocol.

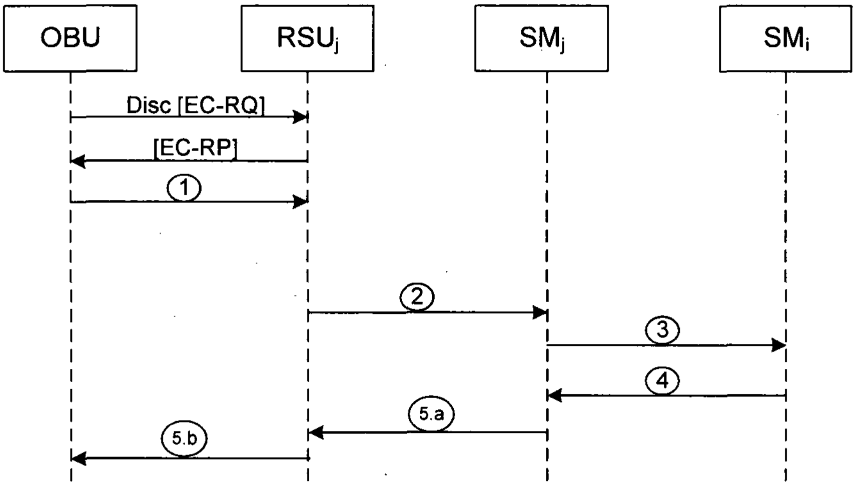

Figure 7.3 - EC-RQ exchange messages

7.6 Multi-hop initiation request protocol [MHI-RQ]

This part covers the initial service request protocol suitable for multi-hop environments. For this study, it is considered that there must be an exchange of public keys and validation of digital signatures for intermediate nodes in the multi-hop forwarding. The *MHI-RQ* protocol should follow the same validation steps as those performed in the *SHI-RQ* (see Figure 7.4); however, additional considerations to foster participation among forwarding nodes need to be defined. Notice that services are propagated through intermediate nodes.

A *MHI-RQ* request is first transmitted after a forwarding chain has been established to reach the broadcasting RSU. This forwarding chain consists of all participating nodes which agree to deliver messages between the final recipients up to the fixed network. The establishment of the forwarding chain is assumed to be part of the discovery mechanism in a multi-hop propagation mode within a single district domain. The anchor intermediate node is attached to one RSU, though handover from different RSUs must be maintained.

1. Given the fact that message delivery has to pass through different intermediate nodes, OBU$_i$ sends an encrypted *MHI-RQ* request by using the RSU's public key, previously retrieved during the discovery process, so there is no way for intermediate nodes to retrieve sensitive information from the source. The request message contains the service identifier, protected banking credential and sequence number. Additionally, the source public certificate is appended to the message.

   $$OBU_i \rightarrow OBU_j : Enc\{Srv\_id, Enc\{Bnk\_id\}_{K_{bnk-obu}}, Seq_{OBU_i}\}_{K_{RSU}}, Cert_{OBU_i}$$

2. OBU$_j$ is the anchor node which communicates directly to the broadcasting RSU. OBU$_j$ relays the information received from OBU$_i$ to the local RSU. Recall that intermediate nodes attach their public certificates which will serve at the banking module for the generation of incentives.

   $$OBU_j \rightarrow RSU : Enc\{Srv\_id, Enc\{Bnk\_id\}_{K_{bnk-obu}}, Seq_{OBU\,i}\}_{K_{RSU}}, Cert_{OBU_i}, Cert_{OBU_j}$$

3. The RSU sends a request message to the corresponding SP based on the Service identifier provided by the requester. The SP replies with its public certificate and a sequence number.

   $$SP \rightarrow RSU : Cert_{SP}, Seq_{SP}$$

4. The RSU collects the data coming from the forwarding chain, as well as, the SP and relays the decrypted message to the SM.

   $$RSU \rightarrow SM : Cert_{SP,} Cert_{OBU_j}, Cert_{OBU_i}, Srv\_id, Enc\{Bnk\_id\}_{K_{bnk-obu}}, Seq_{OBU_i}, Seq_{SP}$$

5. The SM creates a new session identifier for the prospective session. Additionally, the SM relays the received the data to the SEC module which contains the public certificates of all participating nodes for their validation. If any holder in the chain of public certificates is found to have a revoked status in the CRL, the processing of the service request is aborted.

   $$SM \rightarrow SEC : Cert_{SP,} Cert_{OBU_j}, Cert_{OBU_i}, SS\_id, Srv\_id, Enc\{Bnk\_id\}_{K_{bnk-obu}},$$
   $$Seq_{OBU_i}, Seq_{SP}$$

6. The SEC module relays the user's banking parameters for their validation at the banking entity.

$$SEC \rightarrow BNK : Cert_{OBU_j}, Cert_{OBU_i}, SS\_id, Srv\_id, Enc\{Bnk\_id\}_{K_{bnk-obu}}, Seq_{OBU\,i}$$

7. In the BKN module, the user will be charged according to the service requested. If validation is successful, the BNK generates credit units for the requester, as well as, the bonus units for each participating node which can serve for later rewards. The credit unit for the user is encrypted by using a pre-established shared secret key while bonus credentials are encrypted by using the public key for each corresponding intermediate node. Additionally, it is generated a transaction identifier and a timestamp.

$$BNK \rightarrow SEC : Cert_{OBU_j}, Cert_{OBU_i}, SS\_id, Srv\_id, Enc\{Bns\}_{K_{OBU_j}},$$
$$Enc\{Crd\_unt\}_{K_{bnk-obu}}, Trn\_id, T, Seq_{OBU\,i}$$

8. The SEC module relays the satisfactory message to the SM. The information intended for the SP is encrypted with a shared secret key between the registered provider and the district security module, while the information intended for the user is encrypted with its public key. This encrypted message included the session key, temporary user ID, encrypted credit units, transaction identifier, timestamp and sequence number. The bonus credential for the intermediate node is appended to the secured composed message. Encryption of the session parameters maintains the integrity of the whole requesting message.

$$SEC \rightarrow_a SM(1) \rightarrow_b RSU : Enc\{Enc\{Crd\_unt\}_{K_{bnk-obu}}, Trn\_id, Seq_{OBU_i}\}_{K_{OBU}},$$
$$PID_1, Dist\_id, SS\_id, Kss, Cert_{OBU_j}, Cert_{OBU_i}, Enc\{Bns\}_{K_{OBU_j}}$$

$$SEC \rightarrow_a SM(2) \rightarrow_b RSU : Enc\{PID_2, SS\_id, Kss, Trn\_id, T, Seq_{SP}\}_{K_{SP}}$$

9. RSU relays session parameters to OBU$_j$ which serves as an anchor point for the multi-hop mode to the fixed infrastructure. OBU$_j$ retrieves its bonus units by decrypting it with its private key.

$$RSU \rightarrow OBU_j : Enc\{PID_1, Dist\_id, SS\_id, Kss, Enc\{Crd\_unt\}_{K_{bnk-obu}}, Trn\_id, T, Seq_{OBU_i}\}_{K_{OBU}}, \\ Cert_{OBU_i}, Cert_{OBU_j}, Enc\{Bns\}_{K_{OBU_j}}, Cert_{RSU}$$

10. The message is forwarded through the multi-hop environment to its final destination. Notice that OBU$_i$ and OBU$_j$ are non trusted intermediate nodes; though they may not share a secret key.

$$OBU_j \rightarrow OBU_i : Enc\{SS\_id, PID_1, Kss, Enc\{Crd\_unt\}_{K_{bnk-obu}}, Trn\_id, T, Seq_{OBU_i}\}_{K_{OBU}}, Cert_{OBU_i}$$

11. On the other hand, the RSU sends the corresponding session parameters to SP which includes the shared session key.

$$RSU \rightarrow SP : Enc\{SS\_id, PID_2, Kss, Trn\_id, T, Seq_{SP}\}_{K_{SP}}$$

Figure 7.4 shows the exchange of messages for the *MHI-RQ* protocol.

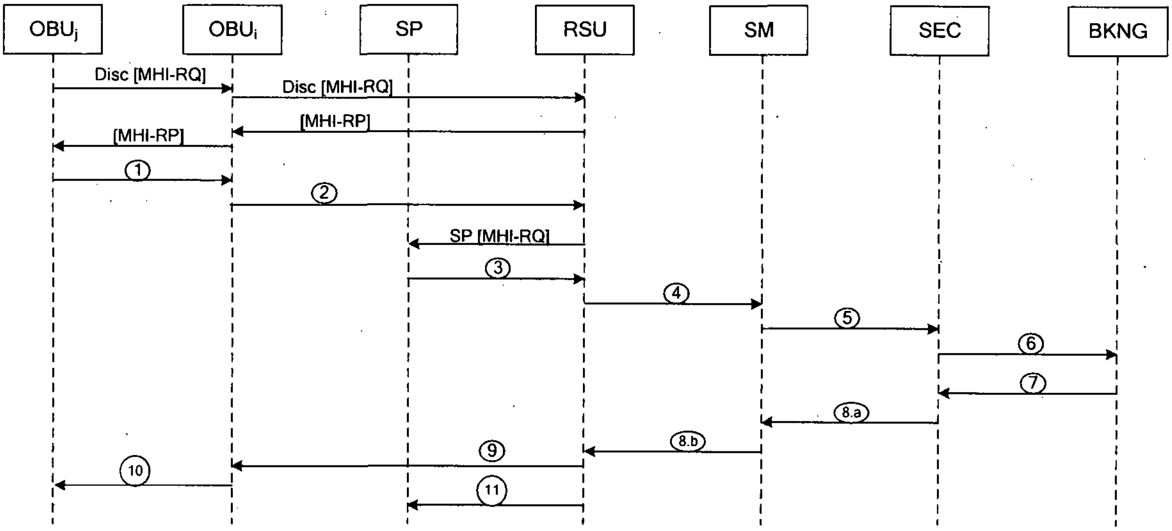

Figure 7.4 - MHI-RQ exchange messages

7.7 Analytical model

In this section, the cost variables are defined regarding data processing to each tier process involved in the district domain architecture, as well as, the link cost for the propagation medium and the cost related to perform cryptographic operations. Table 7.2 enlists the symbols for the corresponding cost values and their definitions.

Table 7.2 – Cryptographic, link and processing costs

Symbol	Definition
w_l	wireless link cost to wireless infrastructure
θ	wired link cost: SP and RSU
ρ	wired link cost: RSU and district domain
w_a	wireless link cost ad hoc medium
α	wired link cost within a district domain
η	wired link cost for domain interconnection
Data access processing cost	
C_1	OBU data access processing cost
C_2	SP data access processing cost
C_3	RSU data access processing cost
C_4	SM data access processing cost
C_5	SEC data access processing cost
C_6	BNKG data access processing cost
Cryptographic cost	
S_{ES}	Encryption cost by using public keys
S_{ET}	Decryption cost by using private keys
S_{DS}	Encryption cost by using secret shared keys
S_{DT}	Decryption cost by using secret shared keys
S_y	Related cost for validating signatures
S_x	Related cost for generating signatures
S_z	Related cost for generating pseudonyms

In the following it is denoted the total signaling cost for each set of request messages.

A. Signaling cost for a *SHI-RQ* message is expressed as:

$$C_{OBU} = 4 * w_l + 3 * C_1 + S_{ET} + S_{DT} + S_X + S_{ES} + S_{DS} \tag{1}$$

$$C_{RSU} = 4 * C_3 + 2 * \rho + S_{ET} + S_{DT} + 2 * S_Y \tag{2}$$

$$C_{SP} = 2 * C_2 + 2 * \theta + S_X \tag{3}$$

$$C_{SM} = 2 * \alpha + 2 * C_4 \tag{4}$$

$$C_{SEC} = 2 * \alpha + 2 * C_5 + 2 \times (S_{DT} + S_{ET} + S_y + S_x + S_z) \tag{5}$$

$$C_{BNKG} = C_6 + S_{DS} + S_{ES} \tag{6}$$

where the total signaling cost for a *SHI-RQ* request becomes as:

$$C_{SHI-RQ} = C_{OBU} + C_{RSU} + C_{SM} + C_{SEC} + C_{BNKG} \tag{7}$$

B. Signaling cost for an *EC-RQ* message is expressed as:

$$C_{OBU_i} = 4 * w_l + 3 * C_1 + S_{ET} + S_{DT} + S_X \tag{8}$$

$$C_{RSU_j} = 2 * C_3 + 2 * \rho + S_{ET} + S_{DT} + S_Y \tag{9}$$

$$C_{SM_j} = 2 * C_4 + 2 * \eta + S_{ES} + S_{DS} \tag{10}$$

$$C_{SM_i} = C_4 + S_{ES} + S_{DS} \tag{11}$$

where the total signaling cost for an *EC-RQ* request becomes as:

$$C_{EC-RQ} = C_{OBU'_i} + C_{RSU_j} + C_{SM_j} + C_{SM_i} \tag{12}$$

C. Signaling cost for a *MHI-RQ* message is expressed as:

$$C_{OBU_i} = 4 * w_a + 3 * C_1 + S_{ET} + S_{DT} + S_X + S_{ES} + S_{DS} \tag{13}$$

$$C_{OBU_j} = 2 * w_l + 3 * C_1 + S_X + S_Y + S_{DT} \qquad 14$$

$$C_{RSU} = 4 * C_3 + 2 * \rho + S_{ET} + S_{DT} + 3 * S_Y \qquad 15$$

$$C_{SP} = 2 * C_2 + 2 * \theta + S_X \qquad 16$$

$$C_{SM} = 2 * \alpha + 2 * C_4 \qquad 17$$

$$C_{SEC} = 2 * \alpha + 2 * C_5 + 2 \times (S_{DT} + S_{ET} + S_y + S_x + S_z) \qquad 18$$

$$C_{BNKG} = C_6 + S_{DS} + S_{ES} + S_{ET} \qquad 19$$

where the total signaling cost for a *MHI-RQ* request becomes as:

$$C_{MHI-RQ} = C_{OBU_i} + C_{OBU_j} + C_{RSU} + C_{SM} + C_{SEC} + C_{BNKG} \qquad 20$$

Notice that the total cost for each signaling protocol becomes the cumulative cost of each participating tier element. A single initial request would have a total cost of $C_{SHI\text{-}RQ}$ to deliver session parameters to the user. In the case of requesting an extension of a service the total cost becomes $C_{EC\text{-}RQ}$. In the multi-hop mode, $C_{MHI\text{-}RQ}$ would represent the total signaling cots for a single service request.

7.8 Mobility model

Given the fact that vehicles can possess high mobility and dynamic behavior, there can be different mobility scenarios which the service district domain has to deal. For instance, if a user gets attached to a RSU that user must be able to request and maintain an on-demand service session within the coverage area. This can be depicted as the case where the vehicle is immobile or travels with low mobility under the coverage of a single RSU. Notice that a service district domain can manage several RSUs under its jurisdiction. Another scenario might be case where there is a transition between adjacent RSUs under the same district domain. Additionally, the interaction between adjacent service districts domains are intended to maintain mid to long-term sessions, so information of active session parameters can be shared through multiple district domains. Finally, a scenario in the multi-hop environment can be considered where a vehicle can request a service session when it is out of the radio transmission coverage of the closest RSU.

For analysis purposes, it is considered the fluid model proposed by [Zhang and Pierre, 2008[1]] in order to deem the mobility behavior of the mobile nodes when traversing through different service coverage areas. The coverage areas are assumed to be circular and contiguous and with a node direction uniformly distributed $[0,2\pi)$ [Nguyen and Harmen, 2001]. First, the border crossing rate out of the coverage area is defined within a single RSU in the incumbent service district domain as expressed in [Wu, 2003]:

$$\mu_s = \frac{\pi v}{4R_s}, \qquad 21$$

where R_s is the radius of the circular area of the transmitting RSU and v is the average vehicle speed. This formula represents the rate when a vehicle is passing through the current coverage area given by the RSU. The border crossing rate out of the serving district domain to an adjacent one is given by:

$$\mu_m = \frac{\pi v}{4R_m}, \qquad 22$$

where R_m is the radius of the serving district domain. The above formula represents the changing rate from one service district domain to the second one. Notice that a service district domain can have multiple RSUs. The border crossing rate for the mobile that stays without changing district domain is given by:

$$\mu_s - \mu_m = \frac{\pi v}{4}\left(\frac{1}{R_s} - \frac{1}{R_m}\right). \qquad 23$$

Now, to evaluate the total signaling cost it is necessary to consider the effect of interdomain mobility which includes the values of the respective border crossing rates (μ_s and μ_m). The total cost expression includes the cost values for executing the *SHI-RQ* and the *EC-RQ* protocols, as well as, the impact of the border crossing rates, vehicle density and the service area.

$$C_T = \rho * A(C_{SHI-RQ} * N * (\mu_s - \mu_m) + C_{EC-RQ} * \mu_m) =$$

$$\rho * A * \frac{\pi v}{4}(C_{SHI-RQ} * N * (\frac{1}{R_s} - \frac{1}{R_m}) + C_{EC-RQ} * \frac{1}{R_m}) \qquad 24$$

where ρ is the vehicle density as defined in [Zhang *et al.*, 2002] for user density, A is the total service area and N is the number of RSUs.

Additionally, it is sometimes useful to introduce the parameter of Session to Mobility Ratio (SMR) given in [Zhang and Pierre, 2008[2]] which is defined as the relation between the session arrival rate and the RSU border crossing rate. This means that the user will be able to request certain number of independent sessions within a district service domain. The SMR is expressed as follows:

$$SMR = \frac{\lambda_s}{\mu_s} \qquad 25$$

Where λ_s is the session arrival rate and μ_s is the RSU border crossing rate.

7.9 Numerical results

For the evaluation of the aforementioned signaling protocols, it is assumed that the related costs in terms of latency (seconds) to estimate the overall signaling cost. The list of the corresponding costs is contained in Table 7.3. Regarding the costs of security operations, benchmark values are provided by Crypto++ [Crypto, 2009] concerning the implementation of cryptographic operations. In the case of digital signatures, these are based on the RSA cryptographic scheme with a fixed length of 128 bytes and for asymmetric encryption/decryption operations it is also considered the RSA (128 bytes) scheme. Moreover, SHA-1 operations are necessary when generating temporary user identifiers/pseudonyms (32 bits) at the security module tier. It is also considered that the AES (128-bit key) mechanism for encryption/decryption when using shared secret keys. Furthermore, it is assumed 20 ms latency for data processing at each tier element and also set the link cost for the wireless medium at 5 ms and for the fixed network at 2 ms.

Table 7.3 – Cryptographic, link and processing values

Symbol	**Value in (s)**
w_l	0.005
ϑ	0.002
ρ	0.002
w_a	0.005
α	0.002
η	0.01
C_1	0.02
C_2	0.02
C_3	0.02
C_4	0.02
C_5	0.02
C_6	0.02
S_{ES}	0.031
S_{ET}	0.007
S_{DS}	0.031
S_{DT}	0.0142
S_y	0.007
S_x	0.0142
S_z	0.044

To evaluate the signaling performance of each protocol it was used MATLAB®. It was observed that in the case of *SHI-RQ*, it would take 0.765 s for a single vehicle to receive a response from a district domain for an initial request made. Notice that this value is the response round trip time for a single access request message. IP assignment is not an issue if IPv6 is used for IP addressing. For the *EC-RQ*, it would take 0.365 s when the vehicle makes a request for extended connectivity to a different district domain. Here, the current session parameters are shared between the session managers of the participating district domains. These results show a slight variation but it can be concluded that cost expressions for the *SHI-RQ* and *EC-RQ* are consistent with the result obtained by the ACE. Now, from the previous values if it is considered a single RSU with a coverage radius of 250 m and a moving vehicle with maximum speed of 40 m/s, then the vehicle would cross approximately the RSU's transmission range (500 m) in 12.5 s. This means that the vehicle would have sufficient time to execute the *SHI-RQ* protocol and retrieve the corresponding session parameters from the district domain. Regarding the *MHI-RQ* protocol it was observed that it would take 0.945 s for a vehicle in a multi-hop transmission mode to request session parameters to the serving district service domain. This latency value includes the participation of only one intermediate node. Results were obtained by using the total signaling cost based on the related cost values of table 7.3.

Figure 7.5 shows the performance of the overall latency for the *MHI-RQ* when the number of intermediate vehicles increases. With a maximum number of 10 intermediate nodes, the latency cost reaches nearly 2.2 s for a single *MIH-RQ* request while for a single intermediate node the latency cost is around .94 s. In this case, the addition of intermediate nodes does not impose a significant impact on the signaling cost since there is only one request at a time being processed by the district domain. However, at the banking module there is more processing operations since bonus units have to be generated for each participating node. Figure 7.6 shows the performance evaluation of the mobility model which includes the corresponding signaling costs for the execution of the *SHI-RQ* and *EC-RQ* protocols. Additionally, it considers the impact of the related border crossing rates with a district domain radius of 1 km and a RSU radius of 250 m. In this graph, it can be observed that when the average speed increases, the border crossing rate for the RSU coverage increases, as well as, the border crossing rate for the district domain. As a result, a vehicle moving at high speeds will need to perform more *EC-RQ* requests since it changes rapidly between contiguous district domains. It can be observed that a cost of 10 s with a vehicle density of 0.0002 (200 vehicles/km^2) is reached with an average speed of 40 m/s. As expected, when the vehicle density increases, the total signaling cost increases. Finally, in Figure 7.7 it is observed the trend for the signaling cost against the SMR which represents the session arrival rate per border crossing rate. The maximum cost value obtained corresponds to a SMR of 30 with vehicle density of 0.0006 and with an average speed of 20 m/s. As expected, when the session arrival rate increases at the district domain, the total signaling cost increases.

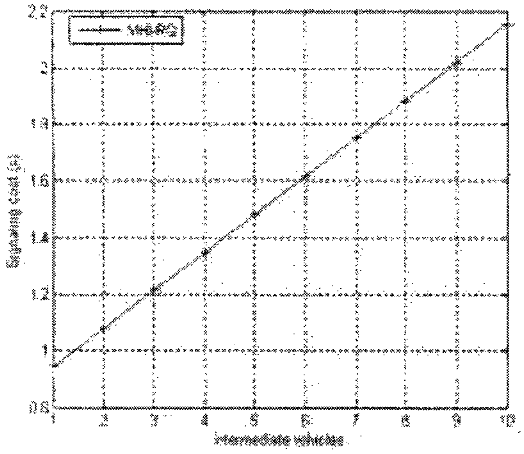

Figure 7.5 - Signaling cost Vs vehicles

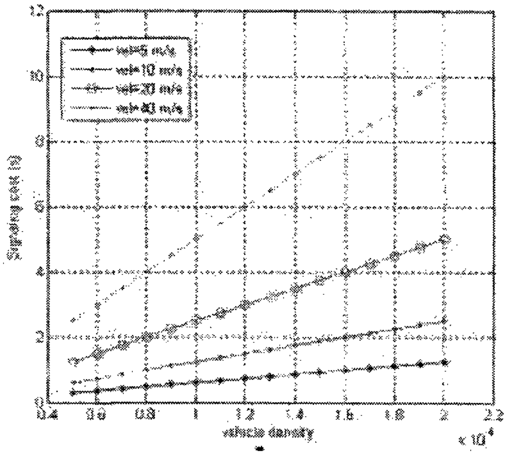

Figure 7.6 - Signaling cost Vs density

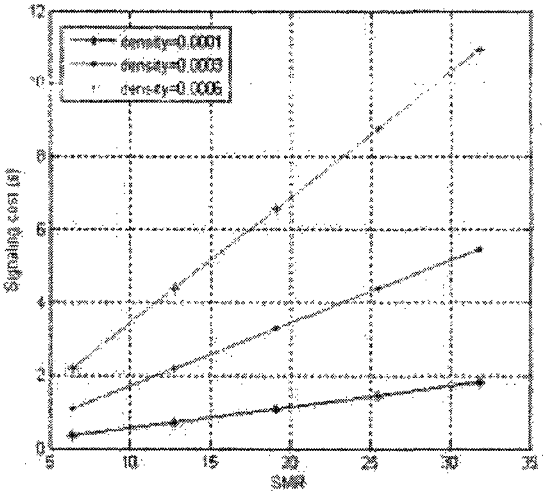

Figure 7.7 - Signaling cost Vs SMR

7.10 Conclusions

Given the fact that commercial roadside service can coexist with the operation of safety messages where safety issues are open for public interest, the same concept can be applied to no-safety applications but with the presence of charging elements in order to generate profits for the providers of the content data, as well as, for the authority of the district domain. For user authentication, the service district domain relies on the verification of certificate revocation lists which will contain the most recent list of certificates which possess a revocation status. Additionally, signature verification is necessary in order to assure that the request message belongs to the holder of the certificate.

In this paper, the analytical model of the secure service district domain architecture has been presented. Three main initiation request protocols are described as *SHI-RQ*, *EC-RQ* and *MIH-RQ*. When a vehicle initiates a request message in the form of a *SHI-RQ* to a specific service district domain through the operating roadside infrastructure, if the validation is successful the user (OBU) will be granted with the corresponding session parameters which includes a temporary session key, as well as, a credential unit issued by the banking module.

When the current user changes from one district domain to an adjacent one, then upon detection of the new district domain an *EC-RQ* message is executed with the objective to trigger the exchange of information between the previous and the new session manager. This means, that on-going session parameters can be extended to other service district domains. Regarding the *MHI-RQ* message, this is executed when the requester vehicle is involved in a multi-hop transmission. At the district domain, the banking module will be responsible for generating credit unit for the requester, as well as, bonus units for each participating node. These banking credentials are encrypted by using the public certificate for each intermediate node. For this study the signaling cost is expressed in terms of latency for *SHI-RQ*, *EC-RQ* and *MHI-RQ* protocols. It was also analyzed the mobility model in order to assess the total signaling cost which involves the signaling within an initial district domain and when the vehicle moves to another domain. This mobility model will depend on the values of border cross rate for staying within the district domain and for moving out the domain. As a result, the obtained values remain acceptable for a reasonable number of vehicles even when increasing the speed.

Finally, interesting research work might be oriented to tackle highly dynamic trajectory patterns in unstable networks, especially when a large number of vehicles are involved and their trajectory patterns become unpredictable. The study of QoS provisioning in ad hoc environments represents a significant challenge regarding the way the packets must be handled and delivered by not trusted intermediate nodes. Additionally, the implementation of secure and robust ad hoc routing protocols would allow an effective forwarding scheme in complex and unstable network topologies. One possible approach is to consider the implementation of secure geographic multicast which guarantees integrity of the data and privacy of the participating nodes without compromising the performance of the system.

Chapter 8 is dedicated to the study of the scalabilty of the service district architecture including different scenarios in a heterogeneous network environment with simulation analysis in terms of the access request time.

CHAPTER 8

JOURNAL OF MOBILE NETWORKS AND APPLICATIONS, SPRINGER

This chapter presents the paper submitted to the Special Issue of Advances and Applications for Vehicular Ad Hoc Networks in Mobile Networks and Applications in Springer 2009. The title of this paper is 'Supporting scalable secure service access for vehicular environments'. This chapter covers scalability with multiple district service domains when a moving vehicle travels from one domain to the other.

8.1 Abstract

8.1.1 Résumé en français

Dans ce travail, nous proposons un modèle pour offrir un service sécurisé quand différents domaines de service successifs sont responsables d'envoyer de paramètres de service aux utilisateurs sur-demande d'une manière dynamique. L'objectif de cette architecture est de faciliter une livraison de service en présence des multiples domaines. Nous avons analysé le temps moyen de réponse pour un utilisateur faisant la demande d'un service sécurisée, de même que, le temps de réponse moyen pour un utilisateur pour avoir accès au service pendant que celui traverse des nouveaux domaines de service dans un environnement de communication hétérogène. L'analyse donne un aperçu sur comment les services sur demande pourront être fournis dans les environnements véhiculaires hétérogènes.

8.1.2 Abstract

Service provisioning elements and different existing approaches intended for vehicular networks were studied in this paper, mainly related to security, accounting models. The purpose of this architecture is to facilitate a scalable delivery of services offered at the roadside infrastructure in the presence of multiple district domains. Through simulations, it is analyzed the average response time for a user to request a secure session, as well as, the average response time for a user to gain this access while roaming across successive new district domains in a heterogeneous environment. The analysis provided a good insight on how secure service provisioning can be implemented in future heterogeneous vehicular environments and what type of challenges need to be tackled.

8.1.3 Index terms

Vehicular networks, service provisioning, security, scalability.

8.2 Introduction

New challenges arise concerning security mechanisms in VANETS which are augmented by the fact that any solution in the transit system needs to be scalable both geographically and with the amount of concurrent users. Most of the solutions might be required to be deployed on heterogeneous environments since different access infrastructure will inevitably coexist along the road. This can be the case of different types of networks such as DSRC, UMTS, WiMAX, GSM, etc. On this regard, the delivery of information for VANETS must be subjected to Quality of Service (QoS) policies to guarantee certain level of bandwidth and network availability. However, QoS parameters satisfaction can be challenging due to the high number of vehicles circulating on the road that are potential consumers of the services offered along the roadside, and also due to their high mobility. In order to maintain a reliable service provisioning, some key factors must be maintained such as low delay, sufficient bandwidth, low jitter, and low loss of information. Adding security mechanisms may typically add delay due to additional treatments, and consume some bandwidth. In the case of vehicular environments, delay can be critical due to the high mobility of vehicles while traversing different networks.

This work addresses scalability issues on the proposed district secure access architecture based on the presence of key modules which provide temporary session parameters for vehicles requesting service access on the road. The architecture can be extended in a scalable way by the interaction of district domains that can comprise heterogeneous wireless technologies. Scalability support will depend on the information shared among multiple service district domains. The results show that the delay introduced by the security mechanisms is acceptable and scales well with the number of vehicles and when different district domains are present. The rest of the paper includes an analysis of multiple service district domains scenario regarding the average service access response time in a scalable heterogeneous topology.

8.3 Secure access for vehicular environments

In general, access schemes are intended to grant network and service access to potential users only if specific access policies and regulations are fulfilled by current requesters. Access control mechanisms promote the development of reliable information service architectures in extended communication systems for scalability purposes. On this regard, significant challenges arise when trying to support scalable service provisioning models in vehicular networks due to the existence of several issues among which there is the potential presence of multiple service providers, network technologies. Additionally, one of the main challenges in vehicular environments is their transitory behaviour which makes it difficult to establish consistent connectivity to wireless fixed infrastructures independently of the user geographical location and/or traffic patterns.

In an on-demand service subscription scheme, the provider has poor or even no knowledge of transitory requesters. For instance, on-demand requests can be pictured in scenarios where the roadside infrastructure advertises information services from specific content providers to potential users. On-demand services can be considered as services that are open to virtually all vehicles that travel in the proximity of an access network where the services are offered. It is clear, however, that exchanges of information between users and providers must be kept reliable and secure in such open-to-all scenario, especially, when sensitive information such as financial transactions is exchanged or when user identities are disclosed. Additionally, when financial transactions take place, such as in a per-use based billing scheme for using services, strict regulations must be complied to and detailed records must be kept regarding all transactions performed. That means that after validations have been completed in the precedent modules, assignation of resources can be issued.

The delivery of information services from the fixed network to vehicles must also support the implementation of Quality of Service (QoS) schemes and policies. The execution of QoS policies defines the way data exchanged as part of the service provisioning, is treated based on its labeled queuing priority and/or assigned bandwidth. These policies can be established when both users and providers respectively agree to provide and accept a specific service level in some so called service level agreement (SLA). The cost related to the type of service level offered may vary such as the better the quality and resources guaranteed, the higher the cost for a service delivery.

User authentication is performed at the security module of the district administrative domain which can comprise multiple certificate authorities and/or their corresponding proxy modules. In the proposed protocol, the authentication of requesters is guaranteed by providing security features during the initial communication setup between users and providers.

Some assumptions have been considered in the architecture. First, the security module must be capable to support and classify different types of requests depending on their priority and/or delay susceptibility. It is worth to emphasize the importance of sorting the type of service that can be delivered by the roadside infrastructure. As aforementioned, the type of priority appended to the service request will determine the level of QoS provisioning. Service policies are contained at the policy module that defines the way a service provisioning must be handled. From the vehicle perspective, there might be some situations where safety-related messages or sensitive-delay data must be treated as fast as possible; so a service taxonomy can allow that safety-related messages be tagged with a higher priority compared to that intended for commercial services.

The authorization process grants resource assignation when validations at the previous modules have been completed. That means that after validations have been completed in the precedent modules, assignation of resources can be issued. Regarding the presence of the session manager, its main function is to retrieve information from the accounting module and establish associations with other external session managers for the purpose of supporting scalability between multiple district domains. Any exchange of information between different district domains will be performed through the interaction of current participating session managers. Session managers can be considered as being the entities responsible of the final stage of the response process to a service request from a vehicle. They assemble all the parameters created for a specific service request before sending back the secure attributes to the corresponding parties.

A single district domain case is a typical case of service deliveries where the vehicle has relatively slow mobility or stays immobile before a nearby roadside unit (RSU) within a single district domain; thus, it can be inferred that the service session can be established along the radio transmission range of the wireless access technology. One of the most likely technologies to be considered for a wide deployment in urban and rural areas is Direct Short Range Communications (DSRC). A feature of this technology is that it supports seven service channels and two control channels used by RSUs to frequently broadcast services offered in an area. This set of services is contained in a list called Provider Service Table (PST). Broadcasting of services can be used in those control channels. Recall that messages can be appended with priority and having top priority those messages labelled as critical.

Even in a single district domain scenario, it is likely that heterogeneous wireless access technologies must be supported in order to provide a scalable service delivery solution that extends over a large geographic area. Therefore, in this scenario, it is considered the general case where different wireless technologies must interact to guarantee continuity on the service.

8.4 Multiple district domains

In mobile environments, it might be situations where vehicles request and get access to a service while moving from one district domain to another while on the road. For this reason, interconnection mechanisms need to be established at many logical levels between neighboring district domains. In particular, it is necessary to put in place mechanisms to facilitate the exchange of information regarding temporary active session registers. This is to allow service parameters from an active session be shared between two concurrent district domains in order to maintain an active session alive without the need for the user to be registered in a new session at the new district domain. If a vehicle is requesting access to a service in a district domain different from the one where the access was initially granted, the current district must contact the previous district in order to retrieve the original user session parameters. This relay based approach allows the user to have continuity in the session parameters when requesting access from a new district domain. The inter-district messages are encapsulated at the transport layer (TCP) and forwarded through the fixed network. Consider a scenario where user A has already been granted access to a service by District$_0$ with all the necessary service attributes as shown in Figure 8.1.

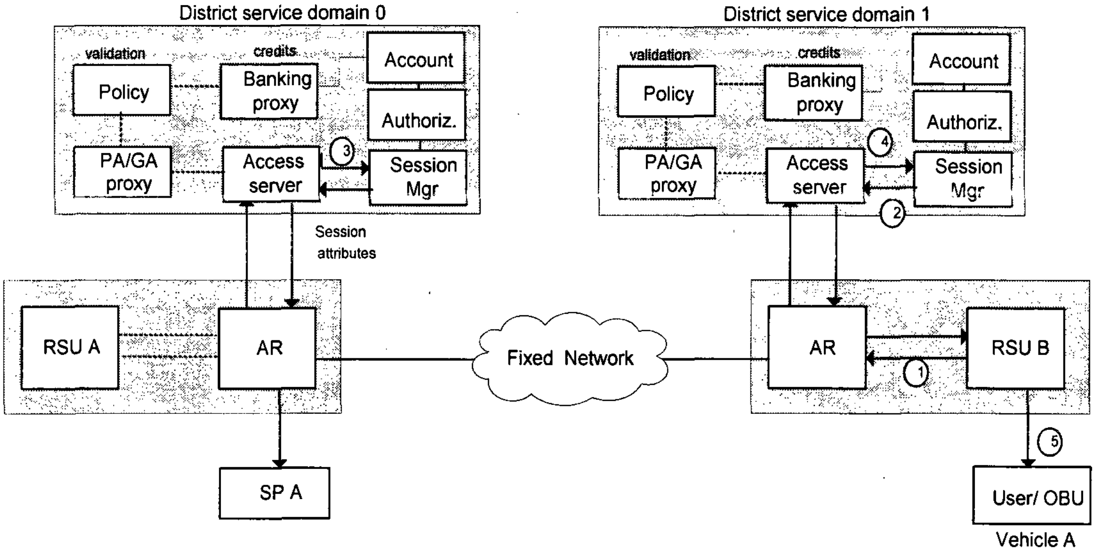

Figure 8.1 - Session parameters exchange between two district domains

When user A moves to District$_1$ while keeping the same service session, the RSU at District$_1$ detects an ongoing session and requests from user A to disclose the corresponding session parameters. In this process, user A sends a signed response message to the new district domain containing its original district identifier, session expiration time, temporary user id (pseudonym), session identifier, transaction identifier and public key certificate (step 1). Additionally, the response message is tagged as an ongoing service session by the RSU. Notice, that this information is independent of the neighbor discovery messages proper to handover operations at the link layer. Once District$_1$ receives the information user *A* through *session manager$_1$*, an encrypted request message is sent to *session manager$_0$* at District$_0$ (step 2). The information contained in the initial request message compromises the claimed session id, temporary user id, district id and user's public key certificate. When *session manager$_0$* receives the request message, the retrieved session identifier is processed to verify the certainty of all the parameters contained in the temporary record at the local accounting module. If the related validation is successful, *session manager$_0$* sends to *session manager$_1$* a success response message along with the active session parameters from the source local register. Then, the information to be shared between the two districts includes the validated session id, temporary user id, service id, transaction identifier, session timestamp and expiration session time (step 3). After this collection of data is done, the response message is encrypted between both districts. Notice that session keys are not exchanged during this procedure since they belong exclusively to the user and the corresponding service provider.

When the response message is received by *session manager$_1$* at District$_1$; the retrieved information is matched with the information disclosed by the user in order to guarantee the certainty of the active session (step 4). If this verification is successful, a new temporary register is created at the local accounting module containing the extracted information. Once validation of all the parameters has been performed, access is granted to the user via the RSU (step 5). For instance, during the validation of the session expiration time values, the original one retrieved from the District$_0$ and the one disclosed by the user are compared. If both values are the same, then the validation succeeds. Otherwise, the validation fails and the user request is rejected.

Regarding banking transactions, the transaction identifier for that specific session is compared to the one retrieved from District$_0$ and the one disclosed by the user. The validation succeeds if both credit identifiers are the same. Otherwise, the validation fails and the user request is rejected. Notice that the session id is kept the same along the duration of the existing session. If a session is terminated, a new access request process and validation has to be performed at the new district domain.

When multiple districts are involved, a chain of relayed districts is formed, i.e. *{District$_i$, Distric $_{i+1}$,..., Distric $_{i+n}$}*. An illustration of this is presented in Figure 8.2, where district domains have to deal with different wireless access technologies. In order to provide more reliable solutions, the service architecture must interoperate regardless of the type of wireless access technology deployed on the road.

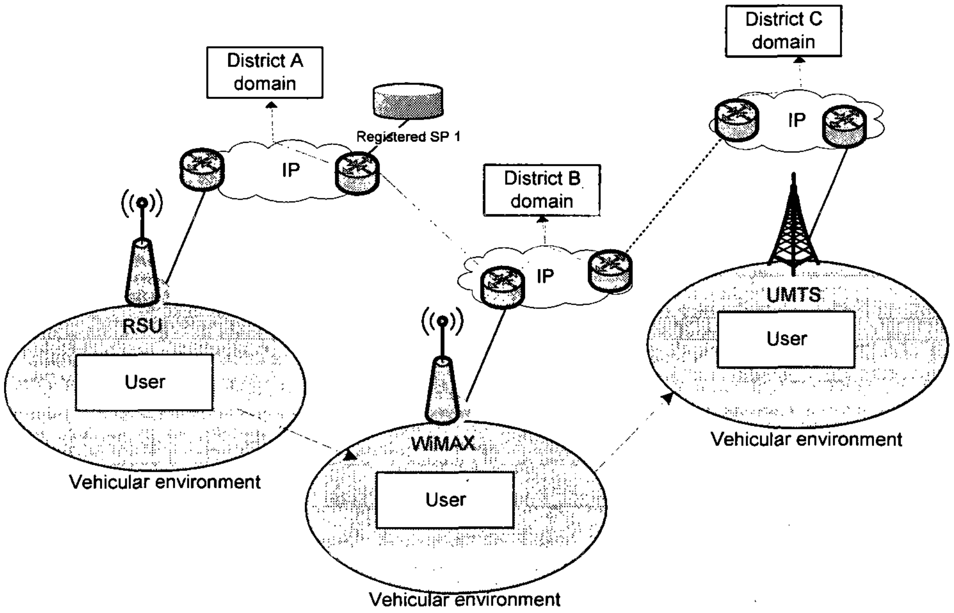

Figure 8.2 - Multiple district domains in a heterogeneous environment

It is worth to emphasize that the active session key is already assigned between the user and service provider from the initial service request to protect any exchange of information between these two entities. Now, when entering to a different district domain, a validation of the current session that the user claims to have needs to be corroborated by the previous district domain. If the validation from the previous district domain is successful, then the new district domain allows access to the transitory user. The communication between district domains is considered to be protected; hence, avoiding any kind of forge of information along the established links between district domains. No need to generate a new set of session keys is required since the information between the service provider and the user is protected by the original session key. Moreover, a user can request a new session at any district regardless of its location without being attached to any one in particular. The process described earlier was intended only to guarantee the continuity of the service parameters upon entering a new district domain without the need to initiate a new request.

8.5 Evaluation of district domains

Introducing security mechanisms, authentication, authorization, and accounting schemes is mandatory for a realistic deployment of service offerings on the road for vehicles. Even though these mechanisms are necessary, a general concern when deploying security mechanism in any architecture is the additional overhead and latency introduced to get access to and to deliver a service. Latency can result from both the additional time required to exchange additional messages, and the processing time required by the communicating entities to make use of those messages. In the case of vehicular environments, getting fast response time becomes particularly important given the speed at which vehicles travel and may room from one network to the other on the road.

For the purpose of analyzing the proposed architecture, the overall schemes of exchanging messages described earlier were implemented in the OPNET® modeler 14.5 wireless suite. It was also considered the cumulative processing time which has to deal with the execution of cryptographic operations at each stage of the communication model. These processing time values were based on the benchmark speeds given in [Crypto, 2009] for different cryptographic schemes as shown in Chapter 6 Table 6.1. The aim is to estimate the total response time during a simulated on-demand request-response process in both single domain and multiple domain scenarios.

For simulation purposes, it was considered a network topology consisting of three district domain representation as shown in Figure 8.3. The core network at each district is implemented as router nodes which interconnect the related district node elements, the service provider and the mobile node. The maximum packet length was set to 1024 bytes and 20 ms latency at each tier process for data processing operations besides the processing time values inherent to cryptographic operations. Though data processing times may vary depending on each tier, this amount of time can be considered reasonable for the scope of this work.

The tool employed to define the access request tier process was the Application Characterization Environment ACE® which is is a robust tool for evaluating the behavior of different tier processes within a network simulation environment. The exchange of request-response messages was implemented as an ACE file and deployed in the network topology. Each tier process in the ACE is assigned to an actual node element in the OPNET project editor for simulation purposes. The statistic results will reflect the effects of the actual response time based on the network topology. Figure 8.4 represents the deployed ACE tier process and which represents the time taken by each tier stage for a session request-response within a single district domain. On the top of the ACE chart, there is a time scale that represents the total elapsed time during the message exchange process. In Figure 8.5, it is shown the ACE tier process corresponding to exchanges between two district domains to relay session parameters.

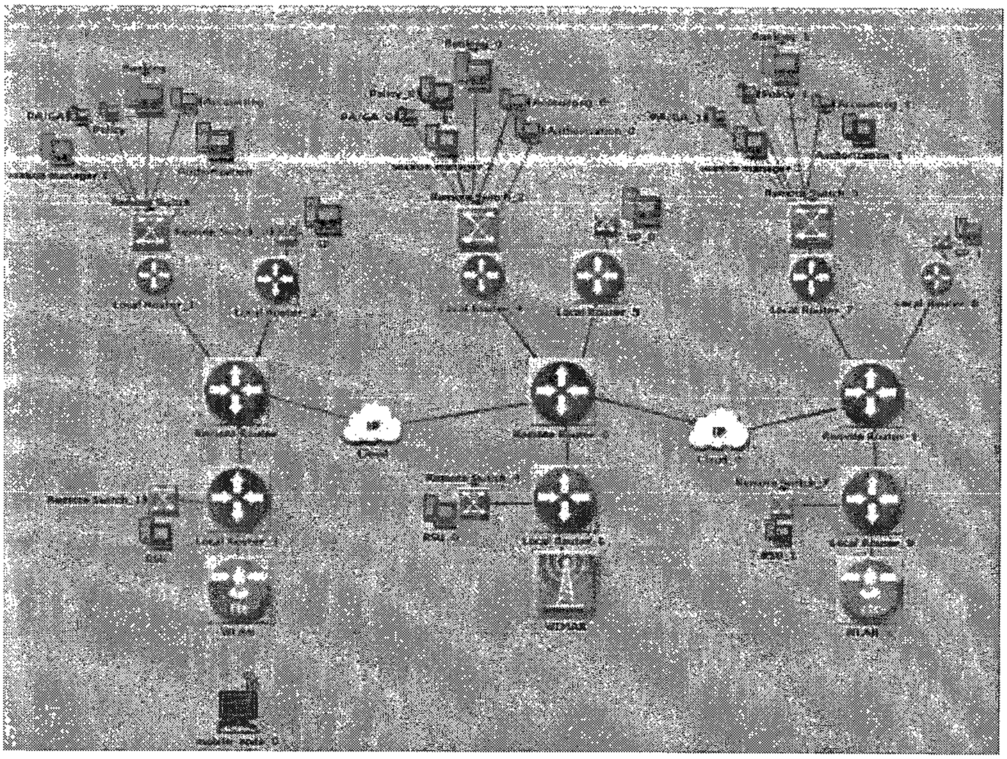

Figure 8.3- Network topology

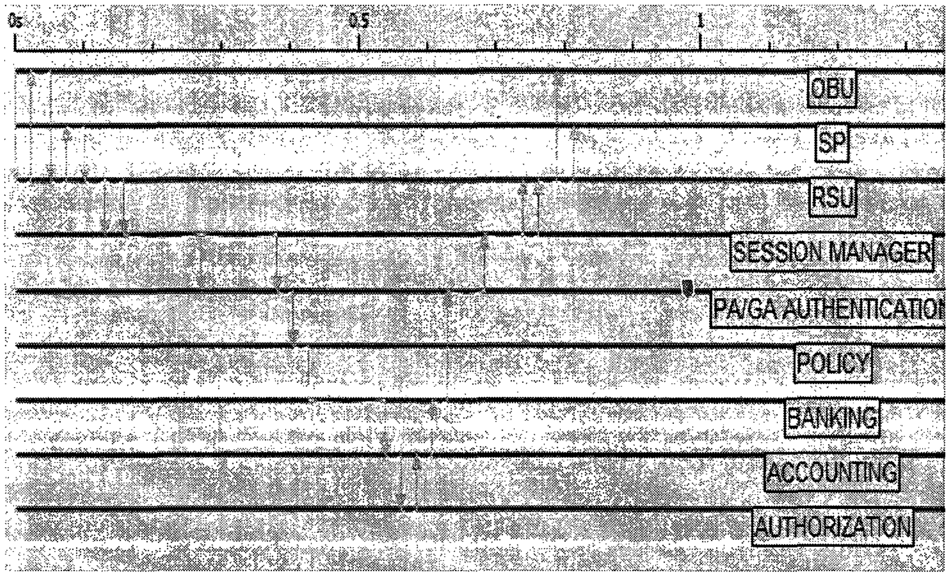

Figure 8.4 - ACE tier process in a single district domain

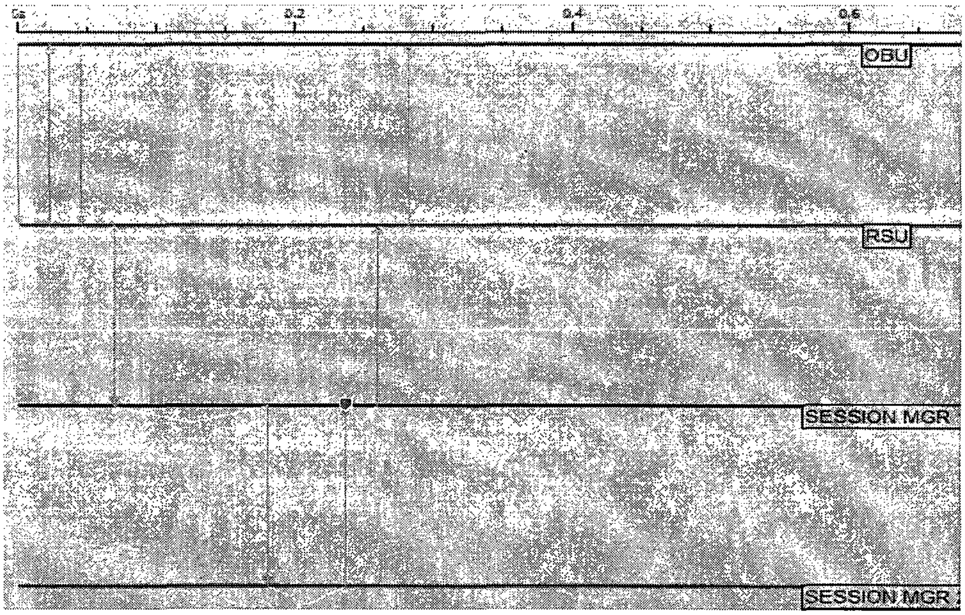

Figure 8.5 - ACE tier process between two district domains

For the network topology in order to represent different wireless access technologies, it was deployed for the first district a WLAN router as an access technology, for the second district a WIMAX base station and for the third one again a WLAN access router. Even though, a district domain configuration is likely to manage many wireless access technologies, in this scenario every district only has one access point/base station. A handover among different access technologies within the same district domain does not involve new authentication/authorization procedures. Therefore it is irrelevant from the point of view of the simulation analysis of the architecture. For simulation purposes auto-assigned IP address are configured for mobile nodes when passing through different subnet.

The objective of the simulations is to estimate the response time it takes for a vehicle to request secure service access within a service district domain, and the response time involved when two and three district domains exchange information. The coverage area offered by each antenna in the simulation is set to 1000 m. First, it was performed sets of simulations for 1, 15, 30 and 80 vehicles by deploying the corresponding ACE process with a total simulation time of 300 s each and with a uniform inter-repetition time between 1 and 3 s. Each vehicle in the simulation was executing new 100 service requests distributed uniformly during the simulation time. More than one service request per vehicle is likely to happen within a time frame, given the fact that for example many embedded systems in future cars may need access to specific independent services. Figure 8.6 shows the average response times for service access for 1, 15, 30 and 80 vehicles. These result times are 0.883 s, 0.888 s, 0.895 s and 1.01 s, respectively. The highest response time is experienced in the 80 vehicles setup while the lowest time values correspond to the single vehicle setup. The difference between the values of one and 30 vehicles varies around 12 ms and does not represent a significant impact on the average response time. However, the maximum response time is reached at the 80 vehicles setup given the increase of the concurrent communicating vehicles. It was noticed that with an even greater number of vehicles the performance of system degrades considerably. Figure 8.7 shows that results for 80 vehicles, it is experienced the highest variation in response time with a maximum peak above 1.25 s. This behavior is given due to an increase in the number of service requests which have to be processed by the simulator concurrently.

The impact of distance was analyzed within the coverage area for a group of 15 nodes which were located at a distance of 400 m from the access point compared to a distance of a few meters close to the access point.

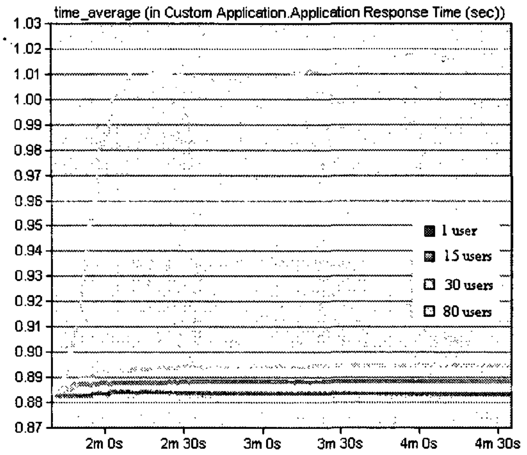

Figure 8.6 - Response time in a district

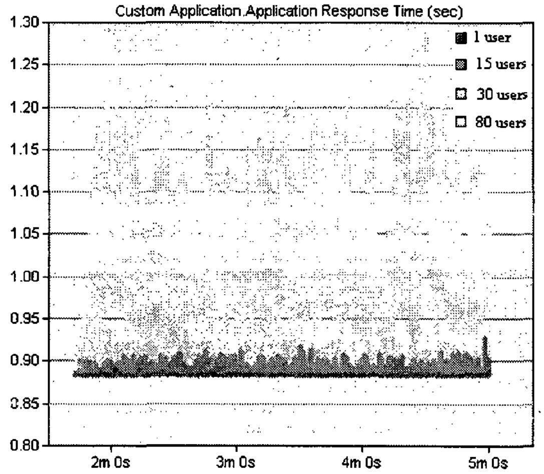

Figure 8.7 - Variation time in a district

Overall, for the single district domain scenario, average response time for a single vehicle remained below 0.89 s. For this time, if it is considered that a vehicle travels at a speed of 100 km/h, the vehicle would have traversed a maximum of 25 m which is smaller than the overlapping zones between any two adjacent coverage areas at both sides of a district domains (15%). Figure 8.6 and 8.7 belongs to WLAN since these results are for the first district domain. The second district domain considers WiMax as an access technology.

The objective of the second set of simulations was to estimate the response time in a multi-district domain scenario. When a change of district domains is performed by a vehicle, a set of messages has to be exchanged between the two district domains. The source district domain and the neighbor district domain need to share information about the current session parameters in order to allow the user to have access to a current service at the new district domain.

For a first simulation setup, it was included the corresponding ACE process for two district domains within the network topology. Additionally, multiple service requests performed uniformly during a total simulation time of 240 s and with a uniformly inter-repetition time between 1 and 2 s. The average response times for service requests performed by 1, 15, 30 and 80 vehicles that remain static at a traversal zone from the first to the second district. To get the average response time from a different access technology a WIMAX router node was deployed as a base station in the second a district domain. Results regarding the WiMax access technologies are related to the extended connectivity between the first district domain and the second one. The response time is retrieved when the mobile node enters into the WiMax domain.

Figure 8.8 shows that the average response times are around 0.47 s, 0.48 s, 0.50 s and 0.57 s, respectively for 1, 15, 30 and 80 concurrent vehicles. The time difference between the highest and lowest time values is about 100 ms. Figure 8.9 shows that the results obtained for 80 mobile nodes presented the highest variation in the response time with a maximum peak response time of nearly 0.8 s. In general, the tier process for a two district domain requires less response time and the processing compared to that obtained for a single district domain.

In the case where a mobile node is moving at a speed of 100 km/h, the effective distance to perform the discovery of the new district domain and the corresponding handover operation would occur at adjacent overlapping zones. The time required to traverse the overlapping zone, 150 m, would be 5.4 s, which is an order bigger than the average response time.

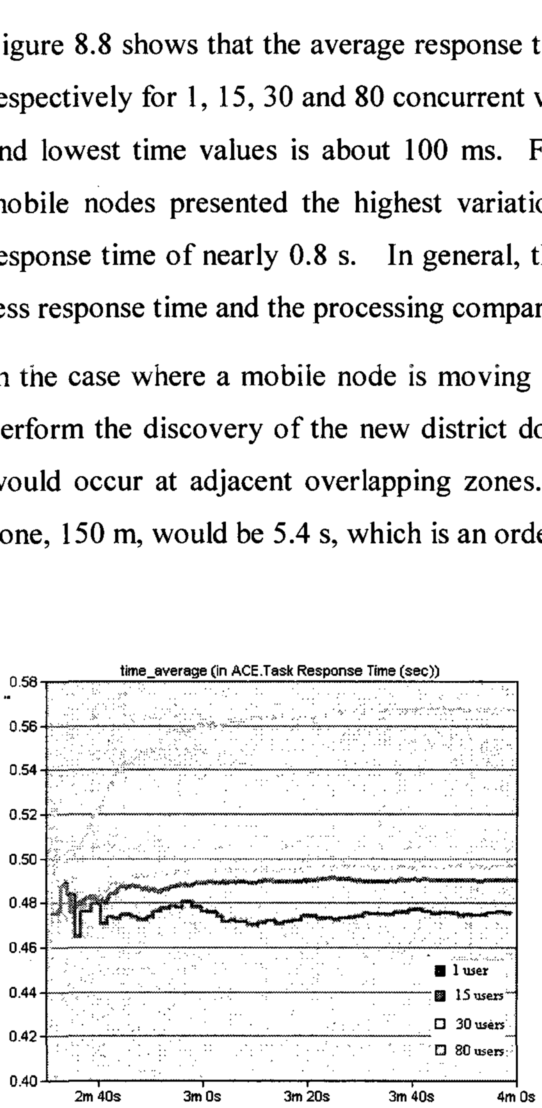

Figure 8.8 - Response time in two districts

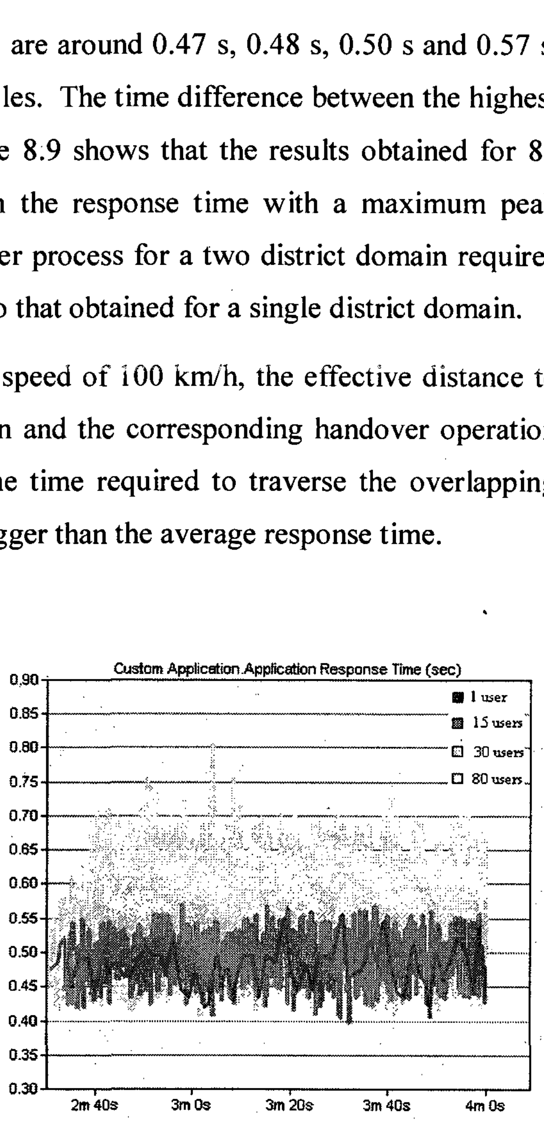

Figure 8.9 - Variation time in two districts

Note that autoassigned IP addressing was configured on mobile nodes. In IPv6 addressing no DHCP infrastructure would be required since the large number of available IP addresses.

The last set of simulations was targeted towards evaluating the average response time when three adjacent district domains are involved in relaying session information. The third scenario depicts the situation were three district domains are present. As a result, three district domains have to share the current session parameters to maintain an ongoing session. This process involves the communication of session information through the core routers between *district*$_2$, *district*$_1$ and *district*$_0$, where the former one is considered the district that issued the original service parameters for a requesting mobile node. A WLAN access point was configured at the last district domain and with the corresponding ACE process for three district domains. Figure 8.10 shows the average response time for requests originating from 1, 15, 30 and 80 coexisting vehicles with time values around 0.57 s, 0.59 s, 0.60 s and 0.65 s respectively. The difference between the single vehicle and the 80 vehicles scenario results is around 80 ms. The results for the 80 vehicles setup experienced the highest variation with a maximum peak of .78 s, as shown in Figure 8.11.

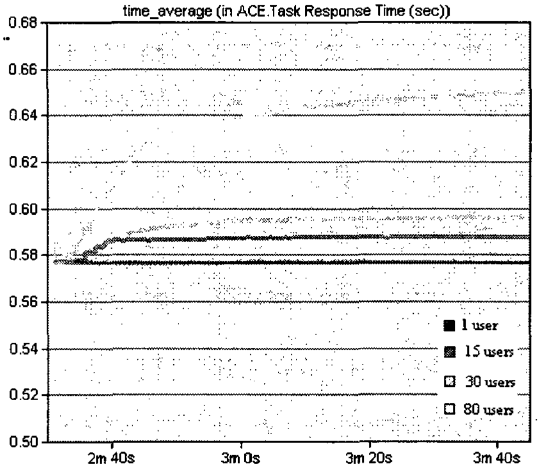

Figure 8.10 - Response time in three districts

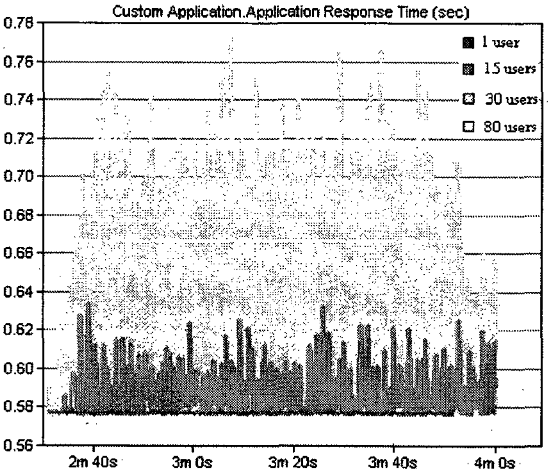

Figure 8.11 - Variation time in three districts

From the results obtained in these simulations, it was observed that the response time values for the generation of service attributes are acceptable in a single district domain for a realistic number of mobile nodes co-existing in an area up to 80 concurrent vehicles per access point. In the case where session parameters need to be shared among multiple district domains, the average response time is also acceptable for sharing session information even when the number of requesters increases. It could also be noticed that the response time values achieved by a single district domain are higher compared to those obtained from two and even three district domains. This is given because the corresponding initial request process for a single district domain involves more tier elements and more processing to set the session parameters. The idea to share and corroborate on-going session parameters between district domains is to avoid the need to request a new service session; therefore, less tier stages and processing is involved.

8.5.1 Discussion

The advantages of implementing robust security schemes for service delivery are evident especially when sensitive information has to be forwarded through unknown and at the same time not trusted vehicles. In this study, it was analyzed the impact of providing secure access in the vehicular context and proposed mechanisms for scalable secure delivery solutions that can guarantee access to on-demand service users while moving through different district domains. On-demand services rely on the premise that vehicles display by nature a transitory behaviour across different district domains where service offering are present. Service providers on the road might have poor or even no knowledge of requesters (vehicles). The simulation studies of the proposed architecture show that the average response time when requesting services on the road would be acceptable for vehicular environments. The response time when multiple district domains are involved also remained acceptable when using two different types of wireless access technologies.

One major issue that must be tackled regarding vehicular environments relates to the high dynamics experienced by ad-hoc vehicle-to-vehicle communication where information services must be delivered beyond the transmission range of any roadside infrastructure. An unstable forwarding topology among vehicles would have a significant impact on service delivery performance to a vehicle beyond the provider. In such a case, long term service sessions between a requester and a provider may not be guaranteed by the service provider or existing networks. In this type of environment it would also be difficult to guarantee QoS parameters to vehicles, and best effort service agreements may be the only types of SLA that would advisably be made available from a service provider to service requesters since service providers cannot guarantee delivery parameters beyond the first hop. The implementation of efficient vehicular ad hoc routing protocols is needed to enable a good service performance, especially, when the delivery of data for the service is delay or bandwidth sensitive. A thorough benchmark study is needed to evaluate the suitability of different existing routing protocols for being used with the proposed architecture in an on-demand service delivery scheme.

8.6 Conclusion

In this paper, relevant characteristics about service provisioning and access architectures in a vehicular context have been presented in multiple district domains. A major concern in vehicular environments is the need to provide robust and secure access to services where reliable delivery of information from providers to vehicles must be guaranteed in a heterogeneous environment.

The service architecture comprises the presence of public and private certificate authorities, session managers, policy entities, accounting, authorization and banking modules within a multiple district domain context. The main goal of the security module is to verify the certainty of the holder's key certificates by using public and private certificate revocation lists. Additionally, the security module generates the corresponding session keys for both the requesting user and the solicited provider. The policy module in the architecture is in charge of defining service policies and regulations. At the banking module, a validation takes place in order to certify that the user's baking credentials can afford the requested service. The accounting module generates a temporary record concerning all the service parameters associated to the transitory user. The authorization module grants resource assignation when validations at the previous modules have been completed. One of the main parts of this architecture deals with the implementation of session managers which are responsible for facilitating the transfer of existing and valid session parameters to other session managers located at different district domains. The communication between session managers helps extend service delivery when a vehicle with an active service session moves to a district domain different from the one where the service parameters where originally received.

The purpose of the presented architecture is to facilitate the delivery of services offered at the roadside regardless of the type of wireless access technologies. It was evaluated the average response time for a vehicle requesting a secure session, as well as, the average response time for a user requesting continuity in access in new district domains in a heterogeneous environment. The results showed that the response time for service access requests are acceptable even when increasing the number of vehicles within the network topology.

The following chapter introduces a service taxonomy for commercial applications such as web, database, voice and video-based applications in a vehicular context and their corresponding simulation results.

CHAPTER 9

SERVICE TAXONOMIES IN VEHICULAR NETWORKS

9.1 Introduction

This chapter presents a service taxonomy for vehicular applications. A description of safety applications is given in section 9.2. Safety applications are considered to have the highest priority level of all incoming and outgoing transmissions of a vehicle. One perspective of service taxonomy is the one based on the Vehicular-infrastructure Integration (VII) for the North American region which is addressed in section 9.3. Another perspective of service taxonomy is the one provided by the CVIS project conceived for the European region also covered in section 9.3.. Since safety applications are not in the scope of the proposed district service architecture, only the implementation of non-safety applications has been studied and analyzed in section 9.4. To evaluate the performance of non-safety applications, simulation scenarios were performed.

9.2 Safety Applications

Safety applications involve the exchange of messages between vehicles or between the infrastructure and vehicles to assist drivers in handling unexpected events on the road, and avoid or minimize the risks of potential dangers. Safety messages can also provide trajectory, status and position information to vehicles in the vicinity with a multi-hop communication [Marousek *et al.*, 2008]. Additionally, communication with the fixed infrastructure can provide additional benefits to improve safety and traffic mobility.

Since safety messages require an efficient delivery of messages of life threatening situations, they must be dispatched with the highest priority. The transmission of safety messages takes place at the MAC level with no further OSI communication layers involved; hence, reducing any additional delay due to the other layers. At the MAC level, efficient communication capabilities are intended to be setup with DSRC/IEEE 802.11p without the common overhead imposed by conventional IEEE 802.11 MAC [Jiang and Delgrossi, 2008].

9.3 Service taxonomy

In this section, two types of taxonomies for application services are addressed. The first one is based on the Vehicular-infrastructure Integration (VII) for the North American region as presented in [Bai *et al.*, 2006] and is described as follows.

1. Safety applications: these applications assist drivers in handling potential dangers on the road.
2. Convenience applications: these applications are related to the handling of traffic management information to maximize traffic flow and traffic throughput.
3. Commercial applications: these applications provide communication services to offer infotainment and informative services to increase driver productivity.

Some applications related to safety messages in [Bai *et al.*, 2006] are described as follows.

1. Stopped or slow vehicle advisor: this type of message is triggered in case of detecting an immobile or slow vehicle that would represent a potential danger for high speed motorists.
2. Emergency electronic brake: this type of message is triggered in case of detecting a sudden stop from the immediate vehicles.
3. V2V post crash notification: this type of message is sent after a collision has been detected to notify oncoming vehicles.
4. Road hazard condition notification: this type of message is sent in case of detecting dangerous conditions on the road.
5. Road feature notification: this type of message informs about traffic conditions on the road.

6. Cooperative collision warning: this type of message is triggered in case of detecting immobile vehicles in the vicinity.

The second type of service taxonomy is based on the Cooperative Vehicle-Infrastructure Systems (CVIS) [CVIS, 2009] for the European region. The main objective of the CVIS project consists of creating a unified technical solution for communication between vehicles and infrastructure by means of an application framework. The CVIS prospected software applications have three main areas:

- Cooperative Urban Applications. The goal is to exchange data between vehicles and RSU from different service providers within urban areas, and create cooperative systems for travel data collection, personalized travel information and traffic management.
- Cooperative Inter-Urban Applications. These applications are intended to provide efficient cooperative services on inter-urban road networks. This will include advanced location techniques for vehicle-infrastructure and vehicle-to-vehicle communications.
- Cooperative Fleet and Freight Applications. These applications target cooperative systems for commercial vehicles offering specific information about actual vehicles position, cargo information, etc. This will result in the optimization of delivery logistics, and the increase of safety and security features for commercial vehicles.

According to the definitions given by the CVIS initiative, safety messages are targeted towards the following usage:

1. Priority Applications. Applications which provide the most efficient mobility to emergency and official vehicles with a possibility to influence green light cycle at traffic lights.
2. Access Control. This is used to improve traffic management and security measures for certain vehicles in real time.
3. Route Conditions. Route notifications about conditions on the road.
4. Speed Alert. Speed limits and warning messages of roadside systems are transmitted to a vehicle to improve traffic safety and compliance.

5. Speed Profile and Advice. A specific speed profile advice is provided to the driver in order to better suit the traffic patterns and thus lower speed fluctuations.
6. Safety warnings. Transmission of relevant applications such as warning about obstacles on the road.

The following table shows the equivalence of applications between CVIS and VII based on safety, speed alerts and road condition awareness.

Table 9.1 – Safety applications for VII and CVIS

Group	North America VII	European CVIS
Safety awareness	Cooperative collision warning	Safety warnings
	V2V post crash notification	Priority Applications
Speed awareness	Slow vehicle advisor	Speed Alert
	Emergency electronic brake	Speed Profile and Advice
Route conditions	Road feature notification	Access control
	Road hazard condition	Route conditions

The taxonomy proposed by the CVIS European initiative for non safety applications seems more detailed than its North American counterpart VII. CVIS gives a more extended categorization for applications feasibility in the urban and inter-urban geographical applications. What is clear however is that both CVIS and VII standard groups envision that safety and non-safety will be deployed using the roadside infrastructure as well as vehicular-to-vehicular communications.

9.4 Non-safety applications

Non-safety applications spam across a variety of services that can provide information or some sort of entertainment to drivers such as web access, streaming audio and video. For instance, navigation assistance can offer real time traffic information to drivers according to their position. Navigation technologies can provide efficient route directions to drivers according to the current traffic conditions. Another type of potential application can be location-based services (LBS) which are used by service providers to offer services to vehicles in the proximity of specific areas. This can be done with the assistance of location servers that record and manage current positioning data [Klimin and Karl, 2004]. Salient elements of LBS are the service discovery protocols whose objective is, on the one side, to enable clients to discover specific service providers in a geographic region and allow, on the other side, service providers to advertise their services in neighboring regions.

According to [Bai *et al.*, 2006] there are some envisioned non-safety applications that can be implemented in vehicular environments:

1. Remote vehicle personalization/diagnostics: downloading or uploading of personalized vehicle settings.
2. Service announcements: announcements of services to vehicles.
3. Internet based applications: web services provided by the roadside infrastructure.
4. Map or database download: vehicles download content from roadside units.
5. Real-time voice and video: transmission and relay of streaming real-time video vehicles or roadside units.

Current research works envision the deployment of IPv6 as the IP addressing scheme to be adopted in vehicles. This is due to the large number of vehicles and network elements that would require an IP address. One solution to provide IP addresses is that vehicles generate their global IP addresses by using their MAC addresses in conjunction with the IPv6 prefix advertised by the current roadside infrastructure [Perera *et al.*, 2006]. The advantages of using IPv6 become evident considering a large number of communicating vehicles in the coming years. The wide supply of IPv6 addresses (128 bits) is enormous compared to that offered by IPv4 (32 bits).

Non-safety applications can be classified depending on the type of delivery they require, i.e. a connection oriented or connectionless based transmissions. The respective transport protocols, TCP or UDP, are directly related to the characteristics and nature of the content data. For instance, for real-time streaming applications the most suitable protocol to use is UDP while for HTTP applications the most suitable transport protocol is TCP. However, generally speaking, vehicular applications that rely on TCP or UDP can be classified in one of the following categories.

1. Database (DB) applications which could represent the access of databases containing specific traffic data from navigation services on the road. This is a connection oriented application type.
2. HTTP applications for web based applications to support mobile Internet on the road. This is a connection oriented application type.
3. Voice over IP for real time applications. This is a connectionless based application type.
4. Video over IP for real time streaming applications. This is a connectionless based application type.

The following table shows the classification of some non-safety applications related to their corresponding type of transport protocol.

Table 9.2 – Classification of non-safety applications

Specific application	Type of application	Type of Procotol
Remote vehicle diagnostics Map/database download Service Announcements	DB	TCP
Internet	HTTP	TCP
Voice	Voice	UDP
Real-time video	Video	UDP

Based on the above classification, we proceeded to the simulation of the performance of the framework proposed in this work in different traffic scenarios in order to assess the behaviour of the architecture in realistic scenarios of vehicular applications.

9.5 Simulations scenarios

To evaluate the performance of commercial non-safety applications, different sets of simulations scenarios were performed by using the OPNET® Wireless Modeler project editor. The objective is to assess the response time for commercial vehicular applications in a service district domain environment. For simulation purposes, applications can be classified as follows.

- Connection-oriented applications: data content applications are included in these sets of simulations such as HTTP and DB applications.
- Real-time steaming applications: for these sets of simulations streaming applications such as IP telephony and video were studied.

9.6 Multidistrict domain scenario

The simulation setup consists of two service district domains configured with WiMAX as the wireless access technology. In a heterogeneous environment, WiMAX can be considered as one of the wireless technologies to cover large transmission areas and which is based on the IEEE 802.16, also called Broadband Wireless Access. In this case scenario, WiMAX is deployed and each district domain contains one base station with a separation distance of 10 km as depicted in Figure 9.1. The mobile node follows a flat trajectory at different speed scenarios of 50 km/h and 100 km/h. The links for the fixed network are configured to be serial link point-to-point (PPP) with a bandwidth capacity of 45 Mbps (DS3).

The multidistrict scenario represents an ongoing session that is being delivered by the first service district domain and needs to be relayed to the following service district domain. A single message request for extended service is executed between the two districts domains before any exchange of payload data can be delivered by the subsequent base station. The main parameter to be analyzed is the packet delay since the delivery time becomes a main constraint in highly mobile environments.

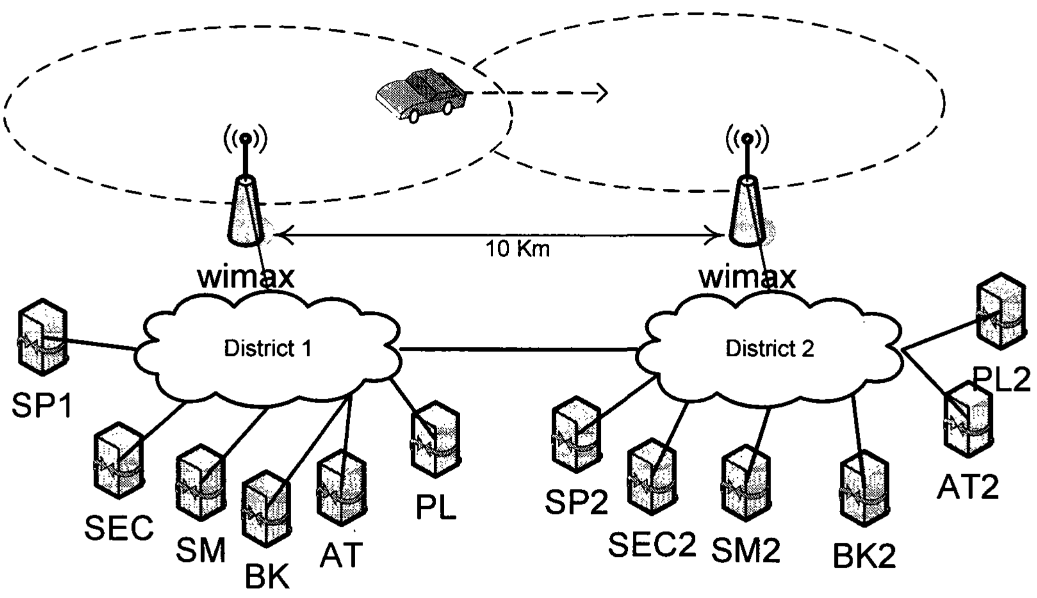

Figure 9.1 Network topology for multidistrict scenario

From Figure 9.1 two independent and adjacent service district domains are depicted. For service district domain 1, the elements are denoted as the security module (SEC); a session manager (SM); banking module (BK); a policy module (PL) and authorization module (AT). For district domain 2 the elements are denotes as follows. A security module (SEC2); a session manager (SM2); banking module (BK2); a policy module (PL2) and authorization module (AT2).

In order to simulate a more realistic network environment, background traffic load was introduced at 30% of the network capacity, that can include traffic such as the one generated by requests and service delivery to multiple vehicles in the area. No priority concerning safety message was configured. Only for the specified application, the type of packet was configured depending on the type of application used.

9.6.1 Database applications

This scenario assesses the end-to-end packet delay for a DB application when an ongoing session is relayed from the first to the second district domains at vehicular speeds of 50 km/h and 100 km/h. The scenario was run 20 times to get the average packet delay from multiple simulation trials. Figure 9.2 shows the average packet delay for a DB application when a vehicle is moving at a speed of 50 km/h. The variance of the results was 0.1x10^{-3}. The ongoing application is subjected to the effects of extended service request messages between district domains before the actual handover could be performed. The relay takes place before 117 s of the simulation time with an increase in the packet delay time. The average packet delay is around 0.03 s with a content data rate of 50 Kbps. The frequent peaks in delays are due to the speed of the mobile node. The average packet loss rate is 0.055. Major packet drops occur in the actual handover from district one to the second district. In Figure 9.3, the speed of the vehicle is 100 km/h and the packet delay trend presents a high concentration of peaks due to the high velocity. The relay takes place at 60 s of the simulation time with a peak at packet delay where the extended service message is released between the two district domains. Again, the average packet delay remains around 0.03 s with a content data rate of 50 Kbps. The worse case occurred at higher speeds since the packet delay shows more variations. The packet delay results obtained are acceptable for the delivery of DB applications even when the service is relayed from one service district domain to the adjacent one. The best performance was obtained with a speed of 50 km/h given that at higher speeds the results present higher packet delay variations along the simulation time. No multihoming is assumed, that is the reason why communications between adjacent session managers is required to extend the service.

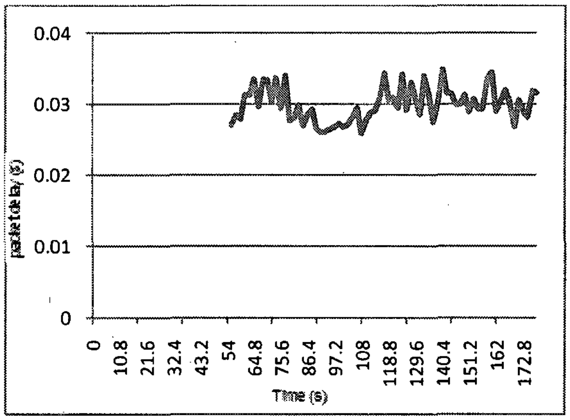

Figure 9.2 - DB packet delay at 50km/h

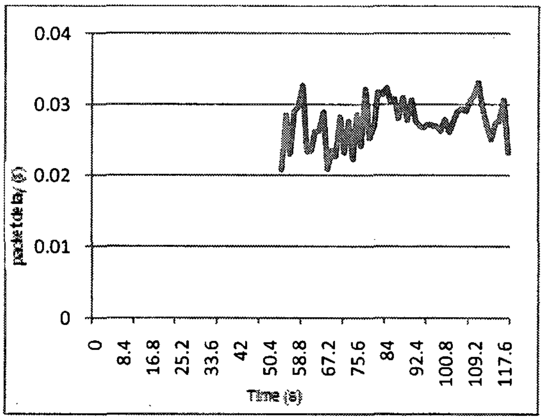

Figure 9.3 - DB packet delay at 100 km/h

9.6.2 HTTP applications

This scenario assesses the end-to-end packet delay for an HTTP application in two district domains from multiple simulation trials. The variance of the rest of results was $0.3\text{x}10^{-3}$. Figure 9.4 shows the average packet delay for a HTTP application when a vehicle moving at a speed of 50 km/h is crossing the border from one district domain to the following one. The relay takes place at 122 s of the simulation time. The average packet delay is 0.15 s with a high content data rate of 200 Kbps. As in the previous DB application, the frequent peaks in delays are due to the speed of the mobile node. The average packet loss rate is 0.053. In Figure 9.5, the speed of the vehicle is 100 km/h and the packet delay trend presents a high concentration of peaks due to the high velocity. The relay takes place at 64 s of the simulation time with an increase in the packet delay of .22 s. The average packet delay remains around 0.15 s for a content data rate of 200 Kbps. The packet delay results obtained are acceptable for the delivery of a HTTP application in multiple district domains. The best performance was obtained with a speed of 50 km/h given that at higher speeds the results present higher packet delay variations along the simulation time.

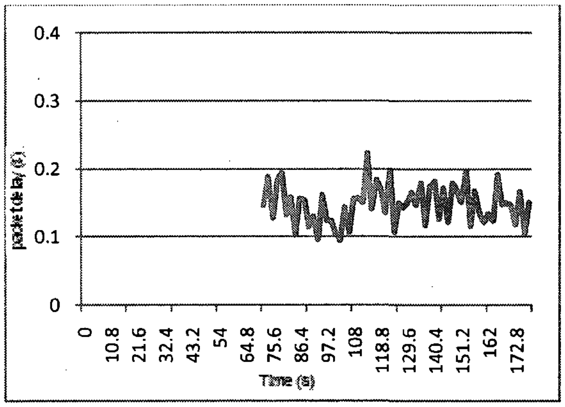

Figure 9.4 - HTTP packet delay at 50 km/h

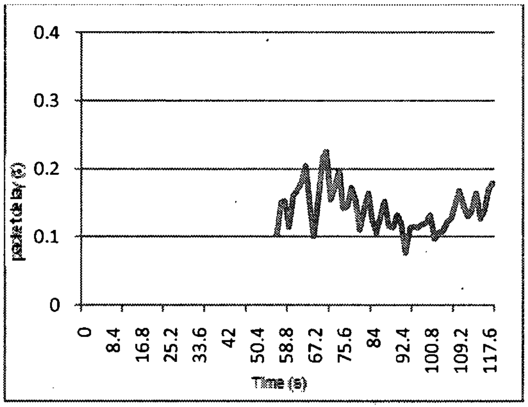

Figure 9.5 - HTTP packet delay at 100 km/h

9.6.3 Voice applications

For real-time streaming applications multiple simulations trials were performed. The variance of the results was a variance of .15x10^{-3}. Figure 9.6 shows the average packet delay for a voice application when a vehicle moving at a speed of 50 km/h is crossing the limit from one district domain. The relay is released at 122 s of the simulation time. The average packet delay is around 0.026 s with a content data rate of 25 Kbps. The average packet loss rate is 0.058. In Figure 9.7, the speed of the vehicle is 100 km/h where the relay takes place at 68 s of the simulation time with a noticeable increase in the packet delay. The average packet delay is around 0.025 s with a content data rate of 25 Kbps. The packet delay results obtained are acceptable for the delivery of a voice application in a multidistrict environment. Again, the best performance was obtained with a speed of 50 km/h given that at higher speeds the results present higher packet delay variations along the simulation time.

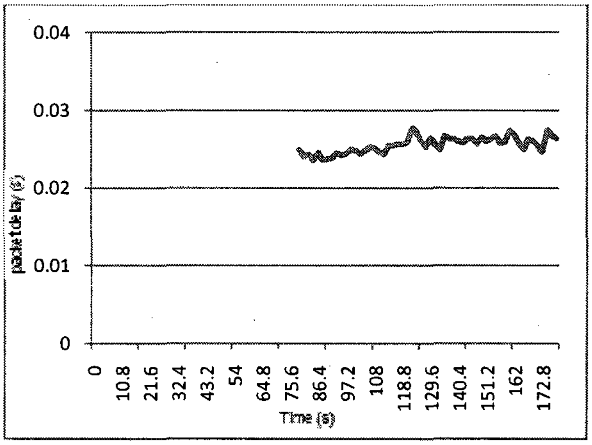

Figure 9.6 - Voice packet delay at 50 km/h

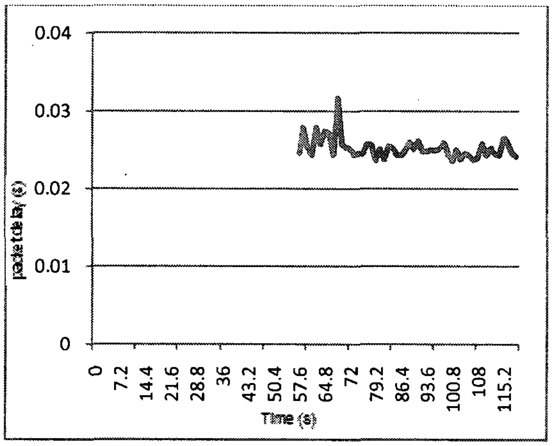

Figure 9.7 - Voice packet delay at 100 km/h

9.6.4 Video applications

This scenario assesses the end-to-end packet delay for a video application when an ongoing session is relayed from the first to the second district domains. Multiple simulations were performed. The variance of the results was .15x10^{-4}. In Figure 9.8, the speed of the vehicle is

50 km/h with a relay of the service at 124 s of the simulation time. The average packet delay is around 0.04 s with a content data rate of 100 Kbps. The average packet loss rate is 0.06. In Figure 9.9, the speed of the vehicles is 100 km/h and the service relay takes place at 67 s of the simulation time. The average packet delay is around 0.04 s for a content data rate of 100 Kbps. The packet delay results obtained are acceptable for a video application when the service is relayed from multiple district domains. The best performance was obtained with a speed of 50 km/h given that at higher speeds the results present higher packet delay variations along the simulation time.

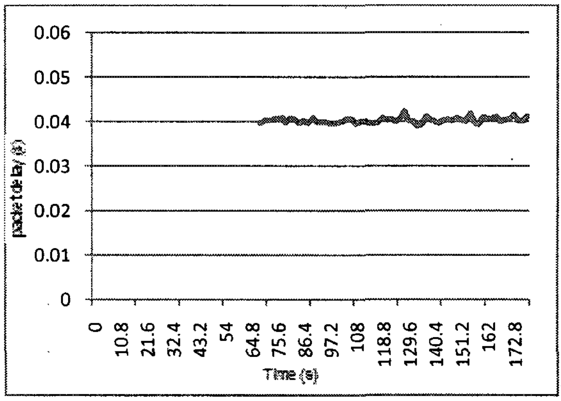

Figure 9.8 - Video packet delay at 50km/h

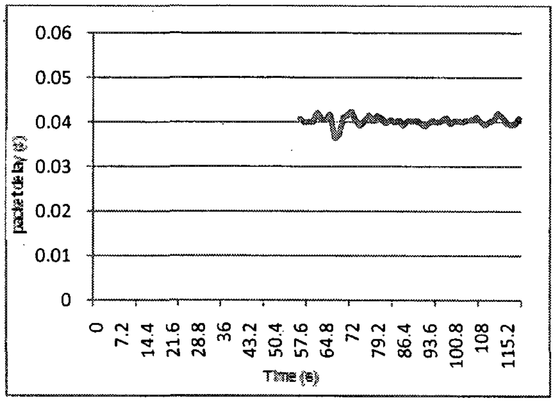

Figure 9.9 - Video packet delay at 100 km/h

As can be noticed in the above graphs for streaming-applications, voice and video, the variation of the packet delay is less compared to those of the connection-oriented applications such as HTTP and DB. Variation in the packet delay has a significant impact on jitter which is an important factor to keep certain level of QoS. The amount of payload traffic is not the same for the applications presented. The delay was end-to-end packet delay (s) one way. Multiple simulations were executed and average to get the end-to-end delay. Notice that video applications should have higher priority since they are delay and jitter sensitive. The data packet was configured as a video-conferencing application. As shown in figure 9.6, 9.7, 9.8 and 9.9 corresponding to UDP based applications jitter is less as expected given it sensitivity to delay variations. Delays are higher for HTTP and DB but are lower for UDP applications. HTTP payload traffic is higher than the rest of the applications.

9.7 Multi-hop scenario

The simulation setup consists of a single service district domain with a type DSRC 802.11 based RSU wireless access technology. The simulation setups are designed to handle 3 then 5 vehicles hopes for multi-hop communication. The coverage area of the RSU is 1 km as shown in Figure 9.10. The elements of the service district domain are denoted as security module (SEC); a session manager (SM); banking module (BK); a policy module (PL) and authorization module (AT). For the communication between mobile nodes, an AODV routing protocol is configured at each mobile node with a forwarding path which introduces additional overhead between adjacent mobile nodes. The nodes implement the security related delays for communication between adjacent nodes. The mobile nodes follow a straight trajectory with a speed of 50 km/h. The links for the fixed network are configured to be serial link point-to-point (PPP) with a bandwidth capacity of 45 Mbps (DS3). The measure concerning the packet loss was considered to be the number of packets received compared to the number of packets sent.

The scenario represents an ongoing session that is taking place in a multi-hop environment in a single service district domain. In order to simulate a more realistic network environment, a background traffic load was introduced at 30% of the network capacity, to simulate on extra load that might be generated by vehicles accessing services in the surrounding areas. Notice that background traffic was considered for the applications response and not in the previous chapters for accessing services.

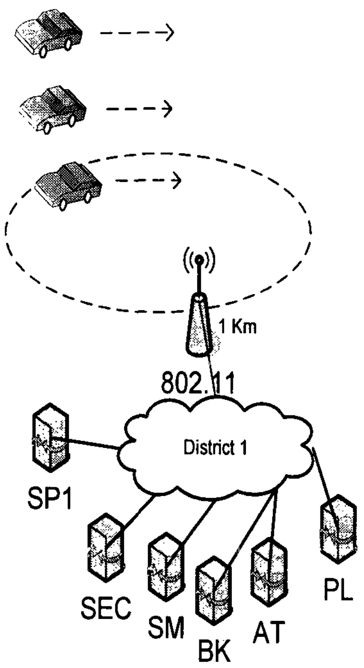

Figure 9.10 - Network topology for the multi-hop scenario

9.7.1 Database applications

This scenario assesses the end-to-end packet delay for a DB application when an ongoing session is forwarded through multiple mobile nodes with a speed of 50 km/h. As in the previous scenario, the simulation setup was run 20 times to get the packet delay average from multiple simulation trials. The variance of the results was 0.4×10^{-3}. The transmission of packets starts after 65 s of the simulation time and when the anchor node is in the coverage area. For this setup, to traverse the RSU coverage area the duration of the session needs to last 50 s. In Figure 9.11, the average packet delay for a forwarding path of three mobile nodes is around 0.17 with some peaks over 0.2 s for an application data rate of 150 Kbps. The average packet loss rate is 0.002. Figure 9.12 shows the average packet delay for a forwarding path of five mobile nodes with higher delays given the presence of more intermediate nodes. The results show an increase in the packet delay up to 0.25 s to reach its destination compared to the delays obtained when three mobile nodes are present. In general, the packet delay results are acceptable even with an increase of intermediate nodes.

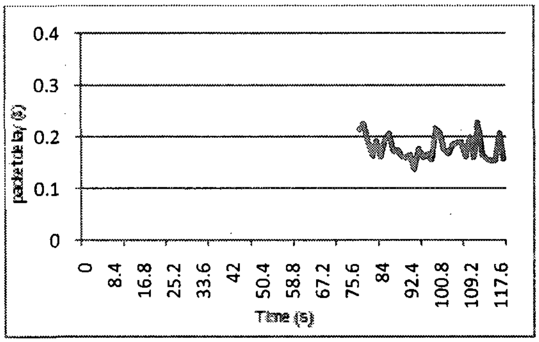

Figure 9.11 - DB packet delay with 3 nodes

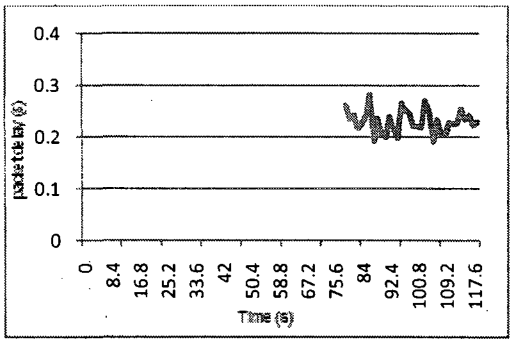

Figure 9.12 - DB packet delay with 5 nodes

9.7.2 HTTP applications

This scenario assesses the end-to-end packet delay for a HTTP application when an ongoing session is forwarded through multiple mobile nodes with a speed of 50 km/h. Multiple simulation trials were performed. The variance of the results was .8x10^{-3}. In Figure 9.13, the average packet delay for a forwarding path of three mobile nodes is 0.10 s for an application data rate of 100 kbps. The packet delay is affected by the presence of intermediate nodes. The average packet loss rate is 0.0022. Figure 9.14 shows the average packet delay for a forwarding path of five mobile nodes. The results show an increase in the packet delay up to .15 s to reach its destination compared to the delays obtained when three mobile nodes are present. Again, the amount of payload traffic is not the same for the applications. In this case the HTTP has higher payload traffic.

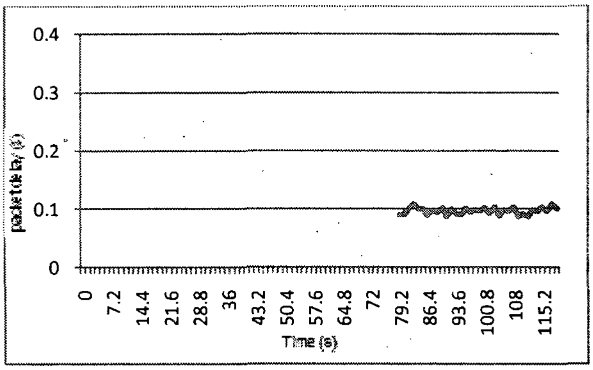

Figure 9.13 - HTTP packet delay with 3 nodes

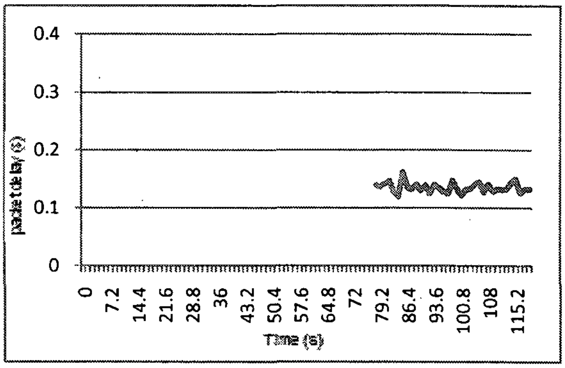

Figure 9.14 - HTTP packet delay with 5 nodes

9.7.3 Voice applications

This scenario assesses the end-to-end packet delay for a voice application through multiple mobile nodes with a speed of 50 km/h. The variance of the results was .3x10^{-3}. In Figure 9.15, the average packet delay for a forwarding path of three mobile nodes is 0.07 s for an application data rate of 50 kbps. The average packet loss rate is 0.0061. Figure 9.16 shows the average packet delay for a forwarding path of five mobile nodes. The results show an increase in the packet delay up to .13 s to reach its destination compared to the ones obtained when three mobile nodes are present.

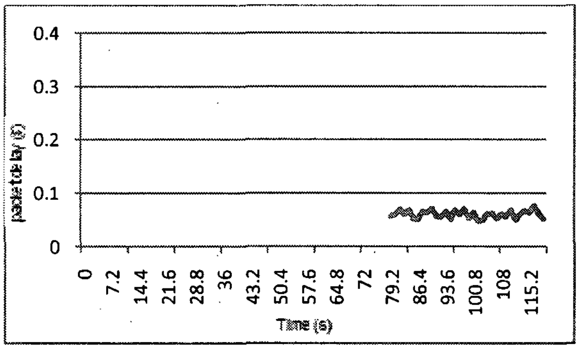

Figure 9.15 - Voice packet delay with 3 nodes

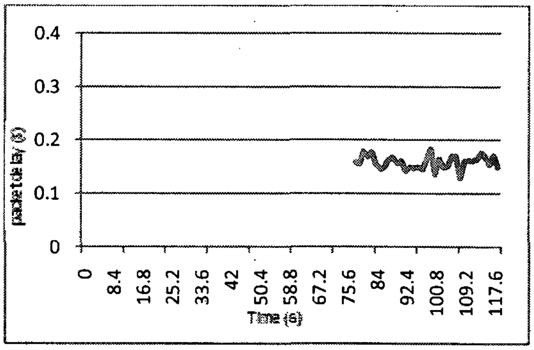

Figure 9.16 - Voice packet delay with 5 nodes

9.7.4 Video applications

This scenario assesses the end-to-end packet delay for a video application when an ongoing session is forwarded through multiple mobile nodes with a speed of 50 km/h. The variance of the results was .39x10^{-3}. In Figure 9.17, the average packet delay for a forwarding path of three mobile nodes is 0.08 s for an application data rate of 100 kbps. The average packet loss rate is 0.0058. Figure 9.18 shows the average packet delay for a forwarding path of five mobile nodes. The results show an increase in the packet delay up to .13 s to reach its destination compared to the delays obtained when three mobile nodes are present.

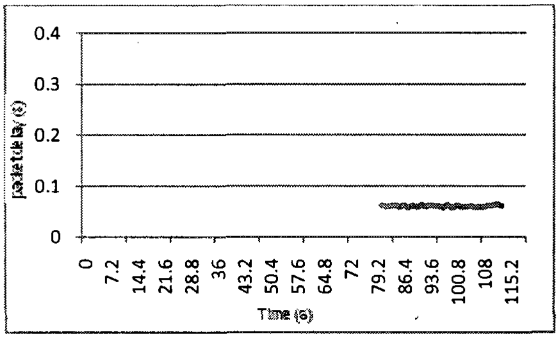

Figure 9.17 - Video packet delay 3 nodes

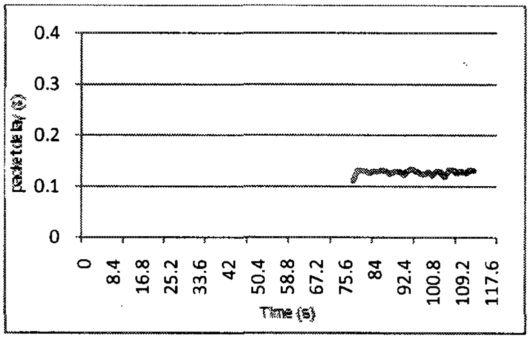

Figure 9.18 - Video packet delay 5 nodes

9.7.5 Discussion

The results obtained for the multidistrict scenarios are acceptable in terms of packet delay when changing between different service district domains. The worse case occurred with speeds of 100 km/h since the packet delay shows more variation in the response of the packet delay. For DB applications, the packet delay results obtained are acceptable for a light payload with a value of 0.03 s. For HTTP heavy applications, the delay was still acceptable with a value of .15 s. For voice applications with a class of voice streaming delivery, the packet delays were acceptable with a value of .025 s and less time response variation. For video applications with a class of streaming delivery with high data rates, the packet delay was acceptable with a value of 0.04 s. Streaming applications are more susceptible to the effects of higher delays and delay variation values given their real-time nature and thus are prone to be affected by network traffic conditions. As shown in figure 9.6, 9.7, 9.8 and 9.9 corresponding to UDP based applications, jitter is less as expected than TCP applications given it sensitivity to delay variations.

The results obtained for the multi-hop scenarios are also acceptable in terms of packet delay even when an increased number of intermediate nodes. As expected, the worse case occurred when the number of intermediate nodes increased up to 5. For DB applications, the packet delay results obtained were acceptable for a heavy payload with values of 0.17 s and 0.25, for three and five nodes, respectively. For HTTP moderate applications, the packet delays were acceptable with values of .10 s and .15 s for three and five nodes, respectively. For voice applications with a class of voice streaming delivery, the packet delays were acceptable with values of 0.07 s and .13 s, respectively and with less variation in the response time. For video applications with a class of streaming delivery, the packet delays were acceptable with values of .08 s and 0.13 s, respectively. Voice and video applications must be guaranteed the use of resources even in multi-hop environments. Moreover, video and voice applications should have higher priorities than other type of applications due to their sensitive delay characteristics. Some data content applications could experience higher delays and be less susceptible to higher packet delay variations; however, a reliable and consistent delivery of the transmitted data must be assured. In the case of the first scenario there is an actual handover between the first district domain and the second one while in the multihop scenario there is no handover. Recall that the relay of services between district domains occur at the edge of their coverage areas; hence, there is a significant impact on jitter. Additionally, the two scenarios employ different technologies, in the first one WiMax and in the second one IEEE 802.11, with different packet delays.

9.8 Conclusions

Safety and non-safety applications must coexist for vehicle-to-vehicle (V2V) and vehicle –to-infrastructure (V2I) communications. One major constraint in vehicular environment has to deal with the application response time when facing highly mobility patterns. As explained throughout this chapter, safety applications possess the highest priority to be dispatched and handled by end-users. Moreover, the way services are delivered also depends on the designated class of specific services. As the main objective of vehicular networks is to increase safety measures on the road by giving timely information to drivers, life-threatening messages are given the highest priority and their transfer must be expedited. For non-safety messages, those that belong to infotainment category are given less priority over safety messages. However, real-time applications as video must be given higher priority over other non-safety applications such as web based and database applications. This classification assigned to commercial applications will help maintain certain quality of service when delivering delay sensitive applications. For instance, applications such as voice should possess lower values in packet delay compared to connection based applications but are more susceptible to the current background traffic conditions.

The simulation results showed the impact in the response time for commercial applications when experiencing high mobility behavior. For multi-hop delivery, since vehicles will be equipped with DSRC transceivers for ad-hoc communication, classes and prioritization schemes must be maintained along the forwarding path between intermediate nodes. For multidistrict domains deliveries, the intercommunication between district domains should impose manageable additional minimum delay. Again, classes and prioritization of services must be maintained when there is a relay of services from different service district domains. The future of information services offered on the road will depend on the reliability of services even when experiencing highly dynamic environments.

CHAPTER 10

CONCLUSIONS AND FUTURE WORK

In this thesis project key characteristics and models for service environment in the vehicular context have been presented. The major concern was to provide a robust and secure transfer of information between a vehicles and a provider in a spontaneous on-demand manner. The extended secure service provisioning architecture comprises the presence of public and private certificate authorities collocated with accounting and banking entities interacting in active district domains. The main task of the security module is to verify the credentials of the holder's key certificates by using certificate revocation lists. The security module must generate the corresponding secure attributes for the user and the service provider as well.

The simulation results showed that the delay due to security mechanisms was acceptable for both single-hop and multi-hop scenarios even when vehicles travel at high speeds. For multidistrict domains deliveries, the intercommunication between district domains should impose manageable additional minimum delay. For multi-hop delivery, since vehicles will be equipped with DSRC transceivers for ad-hoc communication, low latency should be maintained along the forwarding path between intermediate nodes. Efficient forwarding schemes should be advised among ad hoc vehicular nodes to minimize the number of hops. Different ongoing researches are currently addressing this issue with vehicular routing schemes and broadcasting.

In vehicular environments it is expected that information services may have to be delivered beyond the transmission range of the roadside infrastructure. An unstable forwarding topology among vehicles would have a significant impact on service delivery performance to a vehicle beyond the wireless network. In such a case, long term service sessions between a requester and a provider may not be guaranteed by the service provider or existing networks. One main advantage of the proposed architecture is that it promotes collaboration of forwarding peers by generating incentives in the form of bonus units. The dispatched bonuses foster collaboration in the delivery of information services through a forwarding path.

A primary consideration to bear in mind is that safety applications possess the highest priority when being dispatched and handed to end-users. As the main objective of vehicular networks is to increase safety measures on the road by giving additional information to drivers, life-threatening messages are given the highest priority and their transmission must be expedited. This may of course disturb the delivery of services, but this is of course how it should be. An additional consideration to bear in mind also, is that the way services will be delivered will also depend on the designated class of the specific service. For non-safety messages, those that belong to infotainment category are given less priority over safety messages. However, real-time applications as video are given higher priority over other non-safety applications such as web based and database applications. This classification to specific commercial applications helps maintain certain quality of service (QoS) when delivering delay sensitive applications.

Finally, future research work might be oriented to tackle highly dynamic trajectory patterns in ad hoc networks, especially when a large number of vehicles are involved and their trajectory patterns become unpredictable. The study of QoS provisioning in ad hoc environments represents a significant challenge regarding the way the packets must be handled and delivered by not trusted intermediate nodes. Additionally, the implementation of secure and robust ad hoc routing protocols would allow an effective forwarding scheme in complex and unstable network topologies. One possible approach is to consider the implementation of secure geographic multicast which guarantees integrity of the data and privacy of the participating nodes without compromising the performance of the system.

APPENDIX A

AD HOC ROUTING PROTOCOLS

Delivery of service to a vehicle that is outside the range of RSU needs the help of forwarding strategies in a multi-hop manner across a number of intermediate vehicles. Simulations have shown that the length of a forwarding path is a key factor in service delivery performance in multi-hop scenarios. Routing protocols play an important role in lowering the number of intermediate nodes. It is then worth attention to give an overview on routing that can be used in secure vehicular delivery. Ad hoc routing approaches can be considered as proactive, reactive or hybrid depending on how nodes create and maintain their routing information within the ad hoc environment.

Proactive Routing Protocols

Proactive approaches specify that each node in the network maintains a route to every other route in the network at all times. This process of route creation and maintenance is done by the implementation of periodic and event-trigger updates. The latter consist of the exchange of routing information between nodes given the occurrence of an event. In the case of vehicular scenarios where mobility is a major issue, there is a significant impact in the routing protocol performance due to the frequency of event-triggered updates, especially when mobility increases.

One advantage of proactive approaches is that routes are available the moment they are needed based on a low mobility context. This is because each node consistently maintains an up-to-date route to every other node in the network.

One disadvantage of these protocols is that control overhead can be significant within large networks or in networks where nodes possess high mobility; for instance, case of traffic intersections or highway exits. Therefore, routing information at each node needs to be maintained at all times but present problems to manage scalable networks.

Destination-sequenced distance vector routing (DSDV)

This protocol is based on a distance vector approach which uses node sequence numbers to avoid the counting to infinity problem. Nodes increment their sequence number whenever there is a change in its local neighborhood ensuring the utilization of the most recent information. The routing table contains the destination IP address, destination sequence number, next-hop IP address, hop count and install time. To update the routing information, DSDV uses both periodic and event-triggered routing table updates. For instance, every time interval each node broadcasts to its neighbors its current sequence number along with any routing updates; then, the receiver uses this information to populate its routing table entries using a distant vector algorithm. The updates messages can contain the node's entire routing table or incremental which include only those routing table entries that have changes. The latter is more convenient in order to reduce processing overhead and bandwidth consumption.

Optimized link state routing (OLSR)

OLSR is based on the implementation of multipoint relays (MPRs) in order to reduce the overhead of network floods and size of link state updates, as well. The MPR set is selected such that when a node broadcasts a message, the forwarding of that message by the MPR set will ensure that the message is received by each of its hop neighbors. The MPR set for a given node is the set of neighbors that covers the two-hop neighborhood of the node. Nodes learn their set of two-hop neighbors through the periodic exchange of Hello messages. Each node periodically transmits a Hello message that contains a list of all neighbors. Additionally, there is an association for each neighbor with its directionality. When a node receives this Hello message from each of its neighbors, it obtains complete knowledge of its two-hop neighbor set.

Once each node's MPR set is selected, routing paths within the network can be determined based on any shortest path routing algorithm. Because OLSR is a proactive protocol, each node maintains a route to every other node in the network which might no be suitable for vehicular environments.

Reactive Routing Protocols

Reactive approaches can be considered more suitable to support vehicular environments given that they are intended for on-demand routing; that is, routes are discovered only when they are needed. This is due to the dynamic behavior of vehicles which impacts link connectivity with frequent changes and additional control overhead. For reactive protocols, when a source node needs to send data packets to the same destination, first it checks its route table to determine whether it has a route. If no route exists, it performs a route discovery procedure to find a path to the destination. The route discovery consists of the network-wide flooding of a request message.

One advantage of these approaches is that signaling overhead is likely to be reduced compared to proactive protocols. A drawback might be present when the number of active nodes in the network becomes high; then, the overhead generated by the route discoveries approaches increases considerably which is in part affected by the route discovery latency. This means that the discovery time to find a specific route increases when the number of node increases.

Ad hoc On-demand Distance Vector Routing (AODV)

AODV provides on-demand route discovery in mobile ad hoc networks. Route discovery involves the use of broadcast messages and a unicast reply containing discovered paths. Additionally, AODV relies on node sequence numbers to prevent routing loops and for ensuring selection of the most recent routing path. AODV nodes maintain a route table in which the next hop routing information for destination nodes is stored and maintain. Each routing table entry has an associated lifetime value, however if a route is not used within the lifetime period, the route is expired.

When a source node has data packets to send to some destination, it first checks its route table to determine whether it already has a route to the destination. If such a route exists, it can use that route for data packet transmissions. Otherwise, it must initiate a route discovery procedure to find a route. To start route discovery, the source node creates a route request

(RREQ) message. The message contains the destination's IP address, sequence number for that destination, the source's IP address, current sequence number, a hop count and a RREQ ID. After creating this message, the source broadcasts the RREQ to its neighbors.

When a neigboring node receives a RREQ, it first creates a reverse route to the source node. The node from which it received the RREQ is the next hop to the source node, and the hop count in the RREQ is incremented by one to get the hop distance from the source. In this way, the RREQ floods the network until reaching a route to the destination.

When a node receives a RREQ, it checks whether it has an unexpired route to the destination. A reply (RREP) message is created containing the source node's IP address, the destination node's IP address, and the destination's sequence number as given by the node's route table entry for the destination. As a result, the destination node unicasts the message to its next hop node towards the source node. Once a route is established, it must be maintained as long as it is needed. Because of the mobility of the nodes in highly dynamic scenarios, links along paths are likely to break so an error message is generated (RERR).

Geographical routing protocols

This type of approach is based on the used of actual geographic coordinates through GPS or can be obtained through reference points on some fixed coordinate system like a cellular base station infrastructure. The use of geographical information can allow control packets or data packets being sent in the direction of the destination only if the recent geographical coordinates for that destination are known. This reduces the control overhead generated in the network; however, all nodes must have continual access to their geographical coordinates for these approaches to be useful which can become an issue when the number of nodes increases.

Location aided routing protocol (LAR)

LAR is a reactive routing protocol that uses geographical coordinates to direct route request messages to the previously known location of the destination. The route discovery procedure is based on the creation of route request message (RREQ) for the intended destination. If the source has a route to the destination, then the source calculates the expected zone and the request zone, and places the coordinates of the request zone into the RREQ message. When a neighbor node receives the RREQ, the node first determines whether it lies in the request zone defined in the RREQ. If the node does not lie within the request zone, then it does not process the packet. Otherwise, if it does lie within the request zone, it processes the packet and either rebroadcast it or sends a reply. The advantage of LAR is that the RREQ message is prevented from flooding the entire network because it is intended to areas that are likely to be in route to the destination. In the vehicular context, this type of location routing protocol might be convenient for the implementation of VANETS since vehicles will be equipped with GPS localization systems.

Hybrid routing protocols

Hybrid approaches are characterized by the use of both proactive and reactive routing components which under some circumstances can optimize the discovery of routes among different forwarding areas.

Zone Routing Protocol (ZRP)

ZRP defines a zone whose radius is measured in terms of hops; therefore, each node uses proactive routing within its zone and reactive routing outside its zone. When the node has data packets for a particular destination, it checks its routing table for a route. For intrazone routing, ZRP defines the Intrazone Routing Protocol (IARP). IARP is a link-state protocol that maintains up-to-date information about all nodes within the zone. On the other side, ZRP uses the Interzone Routing Protocol (IERP) for discovering routes to destinations outside of the zone.

For route discovery, the query message is relayed toward peripheral nodes which support interzone routing using routing trees based on the information retrieved from the intrazone topology. After receiving the message, the peripheral nodes check whether the destination lies within their zone. If the destination is not located, the peripheral nodes bordercast the query message to their peripheral nodes. This process continues until either the destination is located; once a node discovers the destination, it unicasts a reply message back to the source node.

Clustering, hierarchical and secure routing protocols

Hierarchical protocols place nodes into groups (clusters) where the control within a cluster can be held and managed by a cluster leader. When a cluster leader already exists, it sends control packets on behalf of their member nodes. The cluster boundaries are based on the transmission range of the cluster leaders. All nodes within a cluster must be within direct transmission range of the cluster leader. Additionally, nodes that are located within the boundaries of multiple clusters are called gateways which serve as routers between two clusters. In order to elect a cluster leader, there might be an election algorithm in which the node with the highest ID within some area becomes the leader for that area.

An advantage of hierarchical protocols is that hierarchy can be used to implement hierarchical addressing schemes. Addresses can be assigned to nodes based on their cluster membership and increasing the scalability of the network. Each cluster becomes a node at the next-highest cluster level. Some of the disadvantages of hierarchical approaches are that it is necessary to keep periodic overhead to create and maintain clusters. This overhead is needed to keep current information about cluster memberships and gateway availability. To overcome this drawback some clustering approaches are based on an on-demand approach; that is clusters are only created when needed. This can be useful in vehicular environments since mobility becomes an issue as well as the signaling messages can be reduced.

To guarantee a secure delivery of messages, ad hoc routing protocols must protect the exchange of control messages for route discovery and route maintenance. For instance, the Ariadne routing protocol assumes that all communicating nodes have secret keys based on a symmetric security model for the exchange of routing updates [Perera *et al.*, 2005]. The main disadvantage of the symmetric scheme is that face scalability problems especially in vehicular environments where the number of active vehicles can be high.

A more appropriate solution for VANETs is the use of mix zones which can be used to assure privacy in location based services. The way to protect the identity of users is by deploying restricted zones where external vehicles do not receive any sensitive information from the users within the zone. In this mix zone, vehicles can get group keys from the RSU within the zone. As a result, each vehicle potentially can deliver secure messages to its peers within the group zone.

APPENDIX B

Access models

In general, Authorization, Authentication and Accounting (AAA) systems are centralized trusted model where security mechanisms are part of a key management system for authentication and authorization purposes. The request for a service sent through the communication link needs to be authenticated to ensure the certainty of the identity that the requester claims to hold. Thus, all messages are validated by authentication mechanisms. Once, the subscriber's authentication is performed, an authorization of resources is granted and a session setup is established according to the requester's profile. Basically, the authorization of the subscriber in vehicular environments includes the authorization to access a radio channel at the RSU, i.e. channel allocation and bandwidth designation, as well as authorization to reach a service application at the provider's application server. Once a requester has been fully authenticated, the provider is able to grant the right to access services. These rights can be issued by using service credentials but some restrictions can be imposed by the specific service policies. Furthermore, one common mechanism to secure the exchange of information at the network layer, i.e. IP applications, is by employing IPSec [Stajano, 2002] (Secure IP) which can protect data into two modalities: as an IP authentication header (AH) which is a supplementary header of the IP datagram; or as an IP Encapsulating Security Payload (EPS) which encapsulates the entire IP datagram ensuring data confidentiality.

The use of monitoring tools, metering and charging techniques to assess the service consumption need to be implemented until the termination of the session. In a context of multiple services supply, each service session is composed with a unique session identifier [Rensing *et al.*, 2002] allowing the service provider to keep control of the current sessions as well as tracking of previous service sessions.

Spontaneous On-demand access

A system capable of supporting spontaneous on-demand services on the road shall be considered to grant access to transitory potential users. For highly dynamic scenarios, it can be assumed that the service architecture has no previous knowledge of the requesters. As a result an authentication process, charging and accounting processes must be performed to dispatch the necessary credentials for the user to retrieve the service. One advantage of on-demand services on the road is that multiple service providers can coexist in the same infrastructure enabling the implementation of an extensive variety of application frameworks.

Kerberos System

The Kerberos system is a network authentication protocol based on the Needham-Schroeder algorithm which provides authentication and key management support [Stajano, 2002]. The system comprises an authentication server (AS), a Ticket Granting Server (TGS) and a Ticket-Granting Ticket (TGT). The AS authenticates the user based on its registers and if this operation proceeds, the TGT issues a ticket to the user which will be used to request a service ticket to the TGS. Regarding the characteristics of tickets, they have a limited lifetime and their objective is that they serve as the credentials to continue the granting process from the AS to the TGS in order to retrieve the service. At the beginning of the user's session, the user has to enter his password so he can communicate with all the servers that the user is authorized to get access. In general, all users need to be registered at the AS and that must have their corresponding unique ID and hashed passwords to be matched in the AS database. Additionally, the AS must share a secret key with each registered resource server which is going to provide the information service. The AS database resides on what is called the "Kerberos master" and all changes to the database must be made on the master computer system. The main limitation of this approach is that it may result in some problems when experiencing highly dynamic changes on the database, especially, when huge database records are intended to be recorded such as the case of vehicular scenarios. In general, this structure is centralized and rigid, thus it can involve certain constraints about scalability issues.

The main characteristics of the Kerberos authentication systems as described in [Stalling, 2006] are the following:

A secret key shared between the user and the AS is the hash of the user's login password. During login, the user asks the AS for a ticket-granting ticket, which he gets in a packet encrypted under the shared secret key. As a part of the login procedure, the user types his password into his Kerberos client software, which hashes it and uses the result to decrypt the AS's packet.

Kerberos offers a centralized security policy management. The AS can be instructed to define which clients are authorized to proceed with their corresponding servers.

Kerberos can provide authentication between different realm domains. This allows a client in one domain to obtain a ticket for a server in an adjacent domain. Domains are arranged hierarchically and an authentication may follow a complex path along the tree. It is needed for all servers to be online before the requested ticket can be issued.

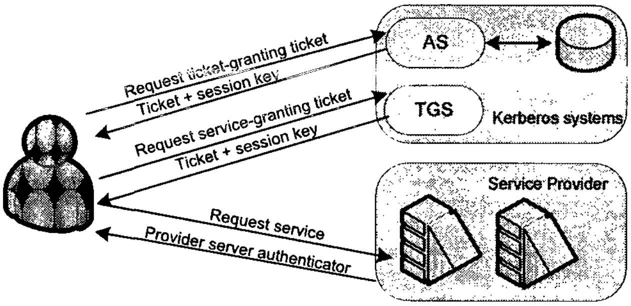

Figure B.1 - Kerberos authentication model

Definition of Kerberos exchange messages

The sequence of messages is depicted in Figure 4.1 and the definition of message is described below based on [Stalling, 2006].

Authentication service exchange

Message 1. Client requests ticket-granting ticket

1. $C \rightarrow AS : ID_C, ID_{tgs}$

Ticket-Granting Service Exchange

Message 2. AS returns ticket-granting ticket

2. $AS \rightarrow C : E(K_C, Ticket_{tgs})$

Message 3. Client requests service-granting ticket

3. $C \rightarrow TGS : ID_C, ID_V, Ticket_{tgs}$

Message 4. TGS returns service-granting ticket

4. $TGS \rightarrow C : Ticket_V$

Client/Server authentication exchange

Message 5. Client requests service

5. $C \rightarrow V : ID_C, Ticket_V$

Discussion on access models

Kerberos is a centralized authentication system based on the generation of ticket services. In order to get access to services the client needs to be registered in the Kerberos database, as well as, the resource servers which will provide the delivery of services. When the client requests some sort of services to the authentication server (AS), if succeeds a ticket-granting ticket (TGT) will be issued to the client who will be included in the request message to the ticket-granting service (TGS). To retrieve the service, the client will disclose the service ticket to the resource server. The Kerberos scheme is based on static registers of clients which in some situations can be less convenient, especially when the database becomes larger or maintenance of the database must be performed. Conversely, spontaneous on-demand services consider the service provisioning of transitory clients even when no previous knowledge is available at the service architecture. For that reason, the service architecture must be based on an authentication scheme based on disclosure of public certificates when if succeeds a session key can be generated for the specific service. Moreover, a billing mechanism has to be defined in order to charge and verify the affordability of the potential user. Temporary registers can be recorded at the accounting module which will keep track of the related parameters issued for the limited session. Another, important element is the session manager which will allow the communication with multiple adjacent service architectures in order to extend an ongoing session. In order to support the delivery of services it would be necessary to design robust service frameworks which will guarantee a secure and efficient operation of service offered on the road.

REFERENCES

Aijaz, A., Bochow, B. and Dotzer, F. (2006) *Attacks on Inter Vehicle Communication Systems – an Analysis*. In proceedings 3rd International Workshop on Intelligent Transportation, Hamburg, Germany.

Antipolis, S. (2005). *Study of a DSRC basic application interface to extend application in vehicles.* In Global Standards Collaboration GSC10. Association of Radio Industies and Business, ARIB Workshop, Angers, France.

Atwood, W. (2007) *An Architecture for Secure and Accountable Multicasting*. In proceedings 32nd IEEE Local Computer Networks, Dublin, Ireland, 73-78 p.

AUTO21®. (2009) http://www.auto21.ca

Bai F., Krishnan H., Sadekar V., Holland G. and ElBatt T. (2006) *Towards Characterizing and Classifying Communication-based Automative Applications from a Wireless Networking Perspective.* IEEE Workshop on Automotive Networking and Applications (AutoNet), San Francisco, USA.

Blum J. and Eskandarian, A. (2004) *The Threat of Intelligent Collisions*. In IT Professional, IEEE Computer Society, 24-29 p.

Buttyan, L. and Hubaux, J. (2003) *Stimulating Cooperation in Self-Organizing Mobile Ad Hoc Networks*. Publisher Kluwer. Mobile Networks and applications, 579-595 p.

Buttyan, L. and Hubaux, J. (2000) *Enforcing Service Availability in Mobile Ad-Hoc WANs*. In 1st IEEE/ACM Workshop on Mobile Ad Networking and Computing, Atlanta, USA.

C. Rensing, M. Karsten and B. Stiller. (2002) *A Survey and a Policy-Based Architecture and Framework.* In IEEE Network, 22-27 p.

Capkun S., Hubaux, J. and Jakobsson M. (2004) *Secure and Privacy-Preserving Communication in Hybrid Ad Hoc Networks.* In EPFL-IC Technical Report no. IC/2004/10.

CVIS, Cooperative Vehicle-Infrastructure Systems, (2009) http://www.cvisproject.org/en/cvis_subprojects., last accessed on February 2010.

Coronado, E. and Cherkaoui, S. (2007) *An AAA study for service provisioning in vehicular networks*, In 32nd IEEE LCN Workshop ON-MOVE, Dublin Ireland, 669-676 p.

Coronado, E. and Cherkaoui, S. (2007) *Secure service provisioning in vehicular networks*, UBIROADS'07, Morocco.

Coronado, E., Cherkaoui, S. (2008) *Service Discovery and Service Access in Wireless Vehicular Networks.* In proceedings of the Global Communications Conference, GLOBECOM, New Orleans, USA.

Coronado, E. and Cherkaoui, S. (2009) *A Secure Service Architecture Support for Wireless Vehicular Networks.* Publisher Journal of Autonomous and Adaptive Communications Systems. Special Issue on: Security, Trust and Privacy in VANETs, January, 136-158 p.

Coronado, E. and Cherkaoui, S. (2009) *Performance Analysis of Secure On-demand Services in Wireless Vehicular Networks.* Publishher Wiley Journal in Security and Communication Networks. September, 114-119 p.

Crypto++, Crypto++ 5.5 Benchmarks, (2007) http://www.cryptopp.com/benchmarks.html, last accessed on May 2009.

DoD Report. (2004) *The DoD Public Key Infrastructure And Public Key-Enabling*, http://iase.disa.mil/pki/faq-pki-pke-may-2004.doc, last accessed on October 2009.

Dotzer, F. (2005) *Privacy Issues in Vanet.* In *Workshop on Privacy Enhancing Technologies*, Dubrovnik, Croatia.

E. Perera, V. Sivaraman and A. Seneviratne, (2005) *Survey on Network Mobility Support.* ACM SIGMOBILE Mobile Computing and Communications Review. Sydney, Australia, 7-19 p.

Eichler, S., Dotzer, F., Schwingenschlogl, C, Fabra, F. and Eberspacher, J. (2004) *Secure Routing in a Vehicular Ad Hoc Network*, IEEE VTC, USA.

El Zarki, M., Sharad, M. and Tsudik, G. (2002) *Security Issues in a Future Vehicular Networks.* In European Wireless.

Ernst, T., Uehara, K. and Mitsuya, K. (2003) *Network mobility from the InternetCAR perspective.* WIDE.

ETC ITS (2008) - http://www.calccit.org/itsdecision/serv_and_tech/Electronic_toll_collection, last accessed on June 2009.

Farradyne, P. (2005) *Vehicle Infrastructure Integration (VII), Architecture and Functional Requirements*, FHWA. ITS-US Department of Transportation.

Festag, A., Fussler, H. et al. (2004) *FleetNet: Bringing Car-to-Car Communication into the Real World.* In Proceeding on the 11th World Congress on ITS, Tokyo, Japan.

Fonseca, E. and Festag, A. (2006) *A Survey of Existing Approaches for Secure Ad Hoc Routing and Their Applicability to VANETs.* NEC Network Laboratories.

Franz, W., Hartenstein, H. and Bochow, B. (2001) *Internet on the Road via Inter-Vehicle Communications.* Workshop der Informatik, Wien, Austria.

Gerlach, M. (2005) *Trusted Network on Wheels.* Publisher ESCAR Embedded Security in Cars, No. 63.

Hartenstein H., Bochow B., Ebner A., Lott M., Radimirsch M., Vollmer D. (2001) *Position-Aware Ad Hoc Wireless Networks for Inter-Vehicle Communications: The Fleetnet Project. ACM* Symposium on Mobile Ad Hoc Networking & Computing MobiHoc 2001, CA, USA, October.

Housley, R. and Aboba, B. RFC 4962, (2007) *Guidance for Authentication, Authorization and Accounting (AAA) Key Management*. Network Working Group, IETF Trust.

Housley, R., Polk, W., Ford, W. and Solo, D. (2002) *RFC 3280. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. Network Working Group. Internet Society.

IEEE (2007) *Trial-Use Standard for Wireless Access in Vehicular Environments (WAVE)-Networking Services*. IEEE Std 1609.3™

J. Choi, M. Jakobsson and S. Wetzel. (2005) *Balancing Auditability and Privacy in Vehicular Networks*. In proceedings Q2SWinet'05, Montreal, Canada.

Karlof, C., Sastry, N. and Wagner D. (2007) *TyniSec: Link Layer Encryption for Tiny Devices.*

http://www.cs.berkeley.edu/~nks/tinysec/, last accessed on December 2007.

Marousek, J., Andrews, S. and Dorfman, M. (2008) *A Comparison of Communications Systems for VII.* Published in Intelligent Transport Systems ITS, NY USA.

Mishra, A. and Nadkarni, K. (2003) *Security in Wireless Ad Hoc Networks*. Published in The Handbook of Wireless Networks, Chap. 3. M. Ilyas, 134-164 p.

Mohan, M. and Joiner, L. (2004) *Solving Billing Issues in Ad Hoc Networks*. In proceedings *ACMSE '04*, Alabama USA.

Moustafa, H., Bourddon, G.and Gourhant, Y. (2005) *AAA in vehicular Communication on Highways with Ad Hoc Networking Support: A proposed Architecture*. In proceedings *VANET'05*, Cologne, Germany.

N. Klimin and H. Karl. (2004) *A hybrid approach for Location-Based Service Discovery in Vehicular Ad Hoc Networks.* In proceedings of Workshop on Intelligent Trasnportation (WIT). Hamburg, Germany.

Nguyen, H. and Harmen, R. (2001) *Performance Analysis of Distributed Location Management for Wireless Networks.* In Proceedings 15th International Conference on Information Networking (ICOIN), Washington, USA.

Obreiter, P., Koning, B. and Klein, M. (2003) *Stimulating Cooperative Behavior of Autonomous Devices*. In proceedings 2nd International Workshop on Wireless Information Systems (WIS2003), Angers, France.

OPNET®, Modeler Wireless Suite, (2008) http://www.opnet.com/solutions, last accessed on March 2010.

Oppliger, R. (2002) *Internet and Intranet Security*. Publisher Artech House, 2nd edition, 92 p.

Papadimitratos, P., Kung, A., Hubaux, J. and Kargl, F. (2005) *Privacy and Identity Management for Vehicular Communication Systems*. Published by eSafety.

Raya, M. and Hubaux, J. (2005) *The Security of Vanet*. In proceeding ACM Security of Ad Hoc and Sensor Networks SASN'05, Alexandria, USA.

Raya, M., Papadimitratos, P. and Hubaux, J. (2006) *Securing Vehicular Communications*. Ecole Polytechnique Fédérale de Lausanne EPFL, Lausanne, Suisse.

Sampigethaya, K., Huang, L., Li, M., Poovendran, R., Matsuura, K. and Sezaki, K. (2005) *Caravan: Providing Location Privacy for Vanet*. In proceedings Workshop on Embedded Security in Cars (ESCAR), San Francisco, USA.

Stajano, F. *Security for Ubiquitous Computing*. (2002) Published by Wiley Series in Communication Networking and Distributed Systems, 179-181 p.

Stalling, W. (2006) *Cryptography and Network Security*. Published by Pearson Prentice Hall, 403-414 p.

TERM (2002) 09 EU – *Transport accident fatalities*. http://www.themes.eea.europa.eu/Sectors_and_activities/transport/indicators/consequences, last accessed on September 2009.

Torrent-Moreno, M. and Hartenstein, H. (2005) *Decentralized Systems and Network Services. Institute for Telematics*, University of Karlsruhe, Germany.

Wu, Z. (2003) *An approach for Optimizing Binding Lifetime with Mobile IPv6*. In proceedings 28th annual IEEE Conference on Local Computer Networks (LCN), Germany, 82 p.

Zhang, L. and Pierre, S. R. (2008) *Performance Analysis of Fast Handover for Hierarchical MIPv6 in Cellular Networks*. In proceedings IEEE Vehicular Technology Conference, Montreal, Canada.

Zhang, X., Gomez, J. and Campbell, A. (2002) *P-MIP:Paging Extension for Mobile IP, Mobile Networks and Applications*. Published by Kluwer Academic Publishers, 127-141 p.

Zhou, D. (2003) *Security Issues in Ad Hoc Networks*. Published in The Handbook of Wireless Networks, Chapter 32. M. Ilyas, 569-582 p.

LIST OF PUBLICATIONS

1. E. CORONADO, S.CHERKAOUI, "Secure service provisioning for vehicular Networks", International Workshop on ITS for Ubiquitous Roads (UBIROADS), Jul. 2007.

2. E. CORONADO, S.CHERKAOUI, "An AAA Study for Service Provisioning in Vehicular Networks", 32nd IEEE LCN 2007, Dublin, 15-18 Oct. 2007.

3. E. CORONADO and S. CHERKAOUI. An IP Connectivity Architectural Model for Heterogeneous Vehicular Networks. In proceedings of the Conference on Parallel and Distributed Computing and Systems, November 12-16 2008, Orlando, USA.

4. A. E. CORONADO, C. S. Lalwani, E. S. CORONADO, S.CHERKAOUI, "Wireless vehicular networks to support road haulage and port operations in a multimodal logistics environment", IEEE SOLI, Beijing, Oct. 12-15th 2008.

5. E. S. CORONADO, S.CHERKAOUI, "Service discovery and service access in wireless vehicular networks", Proccedings of GLOBECOM 2008, New Orleans, Nov.30th-Dec 4th 2008.

6. E. CORONADO,S. CHERKAOUI,"Performance analysis of secure on-demand services for wireless vehicular networks", Journal of Security and Communication Networks, Wiley, September 2009.

7. E. CORONADO, S. CHERKAOUI,"A secure service architecture to support wireless vehicular networks", Special Issue on "Security, Trust, and Privacy in DTN and Vehicular Communications", International Journal of Autonomous and Adaptative Communications Systems (IJAACS), Inderscience, 11 pages, 2009.

8. E. CORONADO, S. CHERKAOUI, “Provisioning of On-demand Services in Vehicular Networks”, Proccedings of Globecom 2009, Honolulu, Nov 30th –Dec 4th 2009.